¿Cuándo está obligado a tener implantada la protección de datos?

Desde Escura hemos ido informando desde nuestra área de Cumplimiento-Protección de Datos, de todas las novedades que desde hace años han entrado en vigor en esta materia.

No obstante, todavía algunas empresas o empresarios individuales nos plantean la conveniencia y/o necesidad de disponer de un sistema implantado en sus empresas y sobre todo de tenerlo **actualizado.**

Es muy recurrente que las empresas hayan implantado un sistema de cumplimiento en materia de protección de datos, pero esta implantación se haya realizado hace años, no está actualizada a las nuevas normativas, ni implantada en los sistemas actuales de la empresa ni formado el personal actualmente en plantilla.

El cumplimiento normativo en el ámbito de la protección de datos es un tema dinámico, que requiere de actualizaciones a las constantes modificaciones normativas y adaptadas a los procesos cambiantes de las empresas.

A efectos recordatorios hemos confeccionado la presente circular que resume cuándo resulta obligatorio tener implantada la normativa de protección de datos en su empresa o actividad profesional, así como el alcance concreto de las obligaciones que le pueden resultar de aplicación. Le adjuntamos, además, una hoja anexa con una tabla resumen de todas las obligaciones, su base legal, el momento en que resultan exigibles y las consecuencias de su incumplimiento.

La regla general: casi nadie queda al margen

El Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) se aplican, desde el primer momento, a cualquier persona física o jurídica —empresa, autónomo, asociación o profesional— que trate datos de personas físicas identificadas o identificables: clientes, empleados, proveedores, usuarios de su web, candidatos a un puesto de trabajo, etc. **No existe un umbral mínimo de facturación, de número de trabajadores o de volumen de datos** que exima a una organización de cumplir la normativa con carácter general: la obligación nace con el propio tratamiento de datos.

Lo que sí varía en función del tamaño, el sector y el tipo de datos tratados es el alcance de determinadas obligaciones concretas (por ejemplo, la designación de un delegado de protección de datos o la realización de una evaluación de impacto), que se detallan en la tabla anexa.

Obligaciones que se aplican prácticamente siempre

- Contar con una base de legitimación válida para cada tratamiento (consentimiento, contrato, obligación legal, interés legítimo, etc.).
- Informar a los interesados, de forma clara y accesible, sobre cómo y para qué se tratan sus datos.
- Implantar medidas de seguridad técnicas y organizativas proporcionales al riesgo (control de accesos, copias de seguridad, cifrado, políticas internas).
- Mantener actualizado el Registro de Actividades de Tratamiento (en la práctica, exigible a la inmensa mayoría de las pymes).
- Atender en plazo los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad.
- Firmar contratos de encargado de tratamiento con todos los proveedores que accedan a datos por cuenta de la empresa.

Obligaciones condicionadas a la actividad o al riesgo

Otras obligaciones solo resultan exigibles cuando concurren determinadas circunstancias: designación de un delegado de protección de datos (sector público, monitorización a gran escala, tratamiento masivo de datos sensibles o pertenencia a alguno de los sectores enumerados en la LOPDGDD), realización de una evaluación de impacto cuando el tratamiento entrañe alto riesgo, garantías reforzadas si se realizan transferencias internacionales de datos fuera del Espacio Económico Europeo, o consentimiento parental cuando se traten datos de menores de 14 años. Todos estos supuestos se detallan, con su normativa y plazos, en el anexo adjunto.

Consecuencias de no tenerla implantada

El incumplimiento de estas obligaciones puede dar lugar a sanciones de la Agencia Española de Protección de Datos (AEPD) que van desde los 40.000 euros en infracciones leves hasta los 20 millones de euros (o el 4% de la facturación anual global) en las infracciones más graves, además de la exposición reputacional y las eventuales reclamaciones de los afectados.

¿Qué le recomendamos?

Le recomendamos revisar, junto con nuestro despacho, el nivel actual de cumplimiento de su empresa a la luz de la tabla anexa, e implantar o actualizar aquellas obligaciones que le resulten de aplicación. Quedamos a su disposición para realizar una auditoría de cumplimiento y acompañarle en su implantación.

ANEXO I
Tabla resumen de las obligaciones en materia de protección de datos

Obligación	Normativa	¿Cuándo es exigible?	Plazo / acción requerida	Consecuencia del incumplimiento
Base de legitimación y principios del tratamiento	RGPD arts. 5 y 6	Siempre que se traten datos de carácter personal (clientes, empleados, proveedores, usuarios web, etc.).	Desde el primer tratamiento de datos.	Infracción muy grave (falta de legitimación): hasta 20 M€ o 4% de la facturación.
Deber de información / transparencia	RGPD arts. 13 y 14	Siempre, en cualquier recogida de datos (formularios, web, contratos, RRHH).	En el momento de la recogida de los datos.	Infracción leve o grave según el caso.
Medidas de seguridad técnicas y organizativas	RGPD art. 32	Siempre, con alcance proporcional al riesgo del tratamiento (contraseñas, cifrado, copias de seguridad, control de accesos).	Implantación y revisión continua.	Infracción grave: hasta 10 M€ o 2% de la facturación.
Registro de Actividades de Tratamiento (RAT)	RGPD art. 30	Obligatorio en la práctica totalidad de los casos. La exención para entidades de menos de 250 empleados solo opera si, además, el tratamiento es ocasional, no entraña riesgo y no incluye categorías especiales de datos: en la mayoría de pymes no aplica.	Elaboración y actualización permanente; exigible por la AEPD en cualquier inspección.	Infracción leve/grave por no poder acreditarlo.
Contratos de encargado de tratamiento	RGPD art. 28	Al contratar proveedores que acceden a datos por cuenta del cliente (gestoría, asesoría, hosting, informática, marketing, mensajería).	Antes de iniciar la prestación del servicio.	Infracción grave.
Delegado de Protección de Datos (DPO/DPD)	RGPD art. 37; LOPDGDD art. 34	Administraciones y organismos públicos. Tratamientos que requieren observación habitual y sistemática de interesados a gran escala. Tratamiento a gran escala de categorías especiales de datos o de condenas/infracciones penales. Sectores con designación obligatoria en España: colegios profesionales, universidades, operadores de comunicaciones electrónicas, prestadores de servicios digitales con elaboración de perfiles, entidades financieras/aseguradoras, distribuidoras de energía y gas, ficheros de solvencia	Comunicar su identidad a la AEPD en el plazo de 10 días desde el nombramiento.	Infracción grave por no designarlo debiendo hacerlo.

Obligación	Normativa	¿Cuándo es exigible?	Plazo / acción requerida	Consecuencia del incumplimiento
		patrimonial, empresas de publicidad y prospección comercial, centros sanitarios, seguridad privada y federaciones deportivas con datos de menores.		
Evaluación de Impacto (EIPD)	RGPD art. 35	Tratamientos de alto riesgo (videovigilancia a gran escala, elaboración de perfiles con efectos jurídicos, tratamiento masivo de datos sensibles, nuevas tecnologías), conforme al listado publicado por la AEPD.	Antes de iniciar el tratamiento.	Infracción grave.
Notificación de brechas de seguridad	RGPD arts. 33 y 34	Ante cualquier incidente de seguridad que suponga un riesgo para los derechos de los afectados (pérdida, acceso no autorizado, ransomware, envío erróneo, etc.).	72 horas a la AEPD; sin dilación indebida a los afectados si el riesgo es alto.	Infracción grave o muy grave.
Atención a los derechos de los interesados	RGPD arts. 15 a 22	Siempre: acceso, rectificación, supresión, oposición, limitación y portabilidad.	1 mes desde la solicitud, prorrogable 2 meses más si es complejo.	Infracción leve o grave.
Transferencias internacionales de datos	RGPD arts. 44 a 49	Cuando los datos se envían fuera del Espacio Económico Europeo (p. ej. herramientas cloud, CRM o email marketing alojados en EE. UU. u otros terceros países).	Garantías adecuadas (decisión de adecuación, cláusulas tipo, BCR) antes de la transferencia.	Infracción muy grave: hasta 20 M€ o 4% de la facturación.
Consentimiento reforzado en menores	LOPDGDD art. 7	Tratamiento de datos de menores de 14 años (por ejemplo, en servicios de la sociedad de la información dirigidos a menores).	Consentimiento de padres o tutores legales.	Infracción grave.