



EL RESPONSABLE DEL TRATAMIENTO

Reglamento europeo de protección de datos (FL18-3061)

Prof. Fernando Cachafeiro



- Cambio sistema de control
- Evaluaciones de terceros
- Responsabilidad proactiva
- Encargado del tratamiento

I. SE HA PASADO DE UN SISTEMA DE CONTROL *EX-ANTE* A UNO EX-POST

- El responsable ha de aplicar medidas técnicas y organizativas adecuadas a fin de garantizar y poder demostrar que el tratamiento es conforma al RGPD
- Hoy ya no es necesaria la inscripción de los ficheros en un registro público

II. CONFÍANZA EN LA EVALUACIÓN DE TERCEROS

- El responsable puede acreditar el cumplimiento del RGPD mediante:
 - a) La adhesión a códigos de conducta (art. 40)
 - *elaborados por asociaciones de organismos responsables*
 - b) Mecanismos de certificación (art. 42)
 - *a cargo de organismos de certificación autorizadas por la autoridad de control*

III. RESPONSABILIDAD (PRO)ACTIVA

- El RGPD establece un catálogo de (nuevas) medidas que los responsables deben aplicar para garantizar tratamiento datos conforme normativa.
- 1. **Análisis de riesgos (art. 35)**
 - *Las medidas a aplicar dependerán del riesgo de los tratamientos que se realizan (i.e. dependiendo naturaleza de los datos, número de interesados, cantidad de tratamientos, etc.)*
- 2. **Registro de actividades de tratamiento (art. 30)**
 - *Recojan los datos básicos del tratamiento (equivalente a la inscripción anterior)*
 - *Exentas entidades menos de 250 trabajadores*

3. Protección desde el diseño y por defecto (art. 25)

- *Antes de comenzar, se deben adoptar medidas que garanticen que sólo se van a tratar los datos conforme al RGPD (i.e. en relación con la calidad de los datos, los tipos de tratamiento, o su accesibilidad).*

4. Medidas de seguridad (art. 32)

- *No todos los tratamientos de datos son iguales*
- *Antes, las medidas de seguridad se establecían en función al tipo de datos que se trataban*
- *Ahora, se tienen en cuenta otras variantes como los riesgos para las personas (tipo de datos, número de interesado, cantidad de tratamientos, etc.)*

5. Comunicación de violaciones de seguridad (art. 33)

- *Cuando se produzca una violación de seguridad, el responsable debe comunicarlo a la autoridad de control (dentro de las 72 horas siguientes)*
- *Cuando entrañe un grave riesgo, también una comunicación a los afectados (art. 34).*

6. Delegado de protección de datos (art. 37)

- *Los responsables que realicen tratamientos a gran escala, deben designar internamente un delegado encargado de supervisar el cumplimiento normativo (compliance officer)*
-

IV. ENCARGADO DEL TRATAMIENTO

- «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- Antes la normativa se centraba en la figura del responsable, ahora contiene obligaciones específicas también para el encargado (art. 28).
- Contrato de encargo: contenido mínimo

V. LISTA DE VERIFICACIÓN

- La AEPD ha publicado una lista de verificación (completa/simplificada) para ayudar a las entidades a realizar una valoración de su situación frente a las obligaciones del RGPD:
https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf