8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Obligaciones de responsables y encargados

Rafael García Gozalo
Jefe del Departamento Internacional

Responsabilidad activa y demostrable

- El Reglamento prevé que los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento
- En otros términos → el Reglamento
  - Considera insuficiente "no incumplir"
  - Incluye obligaciones dirigidas a prevenir incumplimientos
- La no aplicación de estas medidas es sancionable

Responsabilidad activa y demostrable

Tipos de medidas:

- Registro de actividades de tratamiento
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Medidas de seguridad adecuadas
- Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación

Enfoque de riesgo

- Medidas aplicables en función del **riesgo para los derechos y libertades de los interesados**
  - Alto riesgo vs. riesgo estándar
  - El riesgo como criterio de ponderación
- Necesidad de **determinar el nivel de riesgo**

PDdD

- Medidas técnicas y organizativas adecuadas (p.ej. seudonimización, minimización) para aplicar principios de PD de forma eficaz y proteger los derechos
- Integrar las necesarias garantías en el momento de determinar los medios para el tratamiento y en el momento del tratamiento
- Teniendo en cuenta
  - Naturaleza, ámbito, contexto y fines del tratamiento
  - Riesgos de diversa probabilidad y gravedad (no sólo alto riesgo)
  - Estado de la técnica y coste

PDpd

- Medidas técnicas y organizativas apropiadas
- Tratamiento por defecto sólo de datos personales necesarios para cada fin específico
  - Cantidad de datos recopilados
  - Extensión del tratamiento
  - Periodo de almacenamiento
  - Accesibilidad
  - En particular, evitar la accesibilidad a un número indeterminado sin intervención de alguien

Registro de tratamientos

- Obligación para responsable y encargado.
- Contenido (responsable)
  - Identificación y datos de contacto de responsable, corresponsable, representante y DPD
  - Fines
  - Descripción de categorías de interesados y datos.
  - Categorías de destinatarios existentes o previstos (inclusive en terceros países u organizaciones internacionales)
  - TID y documentación de garantías para TID exceptuadas sobre base de intereses legítimos imperiosos
  - Cuando sea posible
    - plazos previstos para supresión de datos
    - descripción general de medidas de seguridad

Medidas de seguridad

- **Responsables y encargados** deben aplicar medidas **técnicas y organizativas apropiadas** para garantizar un nivel de seguridad adecuado al **riesgo**, teniendo en cuenta
  - Estado de la **técnica y costes** de aplicación
  - **Naturaleza, alcance, contexto y fines** del tratamiento.
  - **Riesgos** para los derechos y libertades de las personas
- Reglamento no establece listado estructurado de medidas ni prevé desarrollo o especificación
- La adhesión a un **código de conducta o a un mecanismo de certificación** podrá servir de elemento para demostrar cumplimiento

Notificación de violaciones de seguridad

Notificación a **APD**

- Sin demora y a más tardar en 72 horas desde que se haya tenido constancia. Más tarde, justificación motivada
- No obligación cuando "sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas"
- Reglamento prevé contenido mínimo de notificación
- Documentación de todas las violaciones de seguridad
- Obligación del encargado de notificar sin dilación indebida violaciones de seguridad al responsable

Notificación de violaciones de seguridad

Notificación a **interesados:**

- Cuando es probable que la quiebra entrañe alto riesgo para los derechos y libertades de interesados
- Sin dilación indebida
- Contenido mínimo, que no incluye posibles medidas paliativas
- Excepciones →
  - Implementación de medidas de protección tecnológica que haga ininteligibles los datos a terceros no autorizados (p.ej.: datos encriptados)
  - medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para derechos y libertades
- APD puede obligar a notificar a interesados

Evaluación de impacto PD

- Deberá realizarse cuando sea probable que el tratamiento previsto presente un alto riesgo específico para los derechos y libertades de los interesados, entre otros casos, cuando
  - elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas.
  - tratamiento a gran escala de datos sensibles
  - observación sistemática a gran escala de una zona de acceso público
- Las APD deberán establecer listas adicionales de tratamientos de alto riesgo y podrán establecer listas que no requieren EIPD
- El RGPD prevé un contenido mínimo de la evaluación
- Como novedad, se prevé que habrá de recabarse asesoramiento de DPD y "cuando proceda" la opinión de los interesados

Consulta y autorización previas

- Consulta a APD cuando una EIPD muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo *"y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación"*
- APD podrá →
  - Asesorar por escrito al responsable, y en su caso al encargado
  - Utilizar cualquiera de sus poderes, incluido prohibir el tratamiento
- El derecho nacional podrá establecer consulta y petición de autorización en tratamientos derivados del ejercicio de una misión realizada en interés público por parte del responsable

DPD

- Deberá existir en responsables y encargados cuando
  - tratamiento se realice por autoridad u organismo público
  - actividades principales consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
  - principales consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales
- También habrán de designarlo cuando así lo establezca el derecho de la Unión o de los Estados Miembro

DPD

- Grupo de empresas → Posibilidad de un solo DPD "fácilmente accesible desde cada establecimiento"
- Administraciones Públicas → Un solo DPD para varias entidades
- En otros casos, los responsables, encargados o las asociaciones u organismos que agrupen a categorías de responsables o encargados pueden designar un DPD, que podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados

DPD

- Nombramiento basado en →
  - Cualidades profesionales
  - Conocimientos especializados del Derecho y la práctica en materia de protección de datos atendiendo, en particular a tipo de tratamientos y nivel de protección de cada organización
  - Capacidad para desempeñar sus funciones
- Relación laboral o mediante contrato de servicios
- Compatible con otras funciones, si no hay conflicto de intereses
- No podrá recibir ninguna instrucción en lo que respecta al desempeño de sus funciones
- No podrá ser destituido ni sancionado por desempeñar sus funciones
- Rendirá cuentas directamente al más alto nivel jerárquico
- Podrá ser contactado por interesados y APD

Funciones

- Informar y asesorar sobre obligaciones impuestas por normativa de protección de datos
- Supervisar el cumplimiento de la normativa de protección de datos, incluidas
  - asignación de responsabilidades
  - concienciación y formación del personal
  - las auditorías correspondientes
- Ofrecer asesoramiento sobre EIPD
- Cooperar con la APD y actuar como punto de contacto para cuestiones relativas al tratamiento

Relaciones Responsable – Encargado

- Obligación general de diligencia en selección de encargado.
- Contenido mínimo →
  - Objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos personales, categorías de interesados afectados, obligaciones y derechos del responsable del tratamiento
  - Obligación de tratar los datos únicamente siguiendo instrucciones documentadas del responsable
  - Confidencialidad de personas que manejen datos
  - Medidas “conforme al artículo 32”
  - Contratación de subencargados con autorización previa, general o específica, del responsable, y posibilidad de rechazar subencargados
  - Asistencia al responsable en ejercicio de derechos y en cumplimiento de obligaciones de arts. 32 a 36
- Posibilidad de que Comisión o APD nacionales desarrollen contratos modelo

¡Gracias por su atención!

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es