Principales novedades del Reglamento General de Protección de Datos de la UE

Andrés Calvo Medina
Unidad de Evaluación y Estudios Tecnológicos

Aplicación y armonización

- Será plenamente aplicable el 25 de mayo de 2018
- Reglamento implica una máxima armonización
  - Aplicación directa, sin necesidad de trasposición
  - Desplaza normas nacionales en materias que regula
  - Regulación adicional sólo posible cuando se prevea expresamente

Ambito de aplicación

- Aplicabilidad a responsables y encargados no establecidos en la UE siempre que realicen tratamientos relacionados con
  - La oferta de bienes o servicios (incluidos sin contraprestación económica)
  - El control de su comportamiento
- A personas residentes en la UE

Responsabilidad activa

- 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.
- Tales medidas se revisarán y actualizarán cuando sea necesario

Responsabilidad activa

Tipos de medidas

- Mantener "registro de actividades de tratamiento"
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo Evaluaciones de Impacto

Responsabilidad activa

Tipos de medidas

- Necesidad de autorización o consulta previa con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Violaciones de seguridad de datos personales
- Adopción de códigos de conducta y esquemas de certificación

Medidas de seguridad

- **Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta:**
  - **Estado de la técnica**
  - **Costes de aplicación**
  - **Naturaleza, alcance, contexto y fines del tratamiento**
  - **Riesgos para los derechos y libertades de las personas**

Medidas de seguridad

- Se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia
  - De la destrucción, pérdida o alteración accidental o ilícita de los datos
  - O la comunicación o acceso no autorizados a dichos datos

Medidas de seguridad

- Obligación de incluir en "registro de actividades de tratamiento"
  - Descripción, "cuando sea posible", de medidas de seguridad
- La adhesión a un código de conducta o a un mecanismo de certificación
  - Podrá servir de para demostrar el cumplimiento de los requisitos de seguridad

Relaciones Responsable – Encargado

- Obligación general de diligencia en selección de encargado
- Regulación más detallada que en Directiva:
  - Contrato más detallado
  - Obligación de tratar los datos solo siguiendo instrucciones documentadas del responsable
  - Confidencialidad de personas que manejen datos
  - Medidas de seguridad "conforme al artículo 32"
  - Contratación de subencargados con autorización previa, general o específica, del responsable
  - Posibilidad de rechazar subencargados
  - Asistencia al responsable en ejercicio de derechos y en cumplimiento de sus obligaciones

Relaciones Responsable – Encargado

Algunas peculiaridades:

- Previsión de que el responsable realice auditorías y que el encargado contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable"
- Fin de la prestación implica borrado o devolución de datos, sin incluir transferencia a otro encargado
- Si el encargado infringe las instrucciones recibidas y trata los datos para sus propios fines, se convierte en responsable y sujeto al régimen sancionador
- Posibilidad de "contratos modelo" establecidos por la Comisión

Transferencias internacionales

- Sólo pueden transferirse datos a países que ofrezcan un nivel adecuado de protección establecido por una decisión de la Comisión
- Se amplían y flexibilizan instrumentos de garantía
  - Responsables y encargados pueden ser exportadores
  - Instrumentos jurídicamente vinculantes y ejecutables entre autoridades u organismos públicos

Transferencias internacionales

- Se amplían y flexibilizan instrumentos de garantía
  - BCR (de responsables y de encargados)
  - Cláusulas contractuales estándar aprobadas por la Comisión
  - Cláusulas contractuales estándar aprobadas por una APD nacional y aceptadas por la Comisión
  - Códigos de Conducta y Esquemas de Certificación
- Ampliación de excepciones para casos basados en interés legítimo del responsable

Modelo de supervisión

- Reforzamiento y armonización de APD
- Establecimiento de mecanismos de coordinación y consistencia
- Papel reforzado del Comité Europeo de Protección de Datos
- Complejo sistema de “ventanilla única”
- Compleja regulación de sistema de sanciones

Derechos

- **Transparencia:**
  - **Información concisa, transparente, inteligible, de fácil acceso, lenguaje claro y sencillo**
  - **Especial atención a los menores**
- **Derecho al olvido / Supresión**
- **Derecho a la portabilidad de los datos del interesado**
- **Derecho de indemnización y responsabilidad**

Sanciones

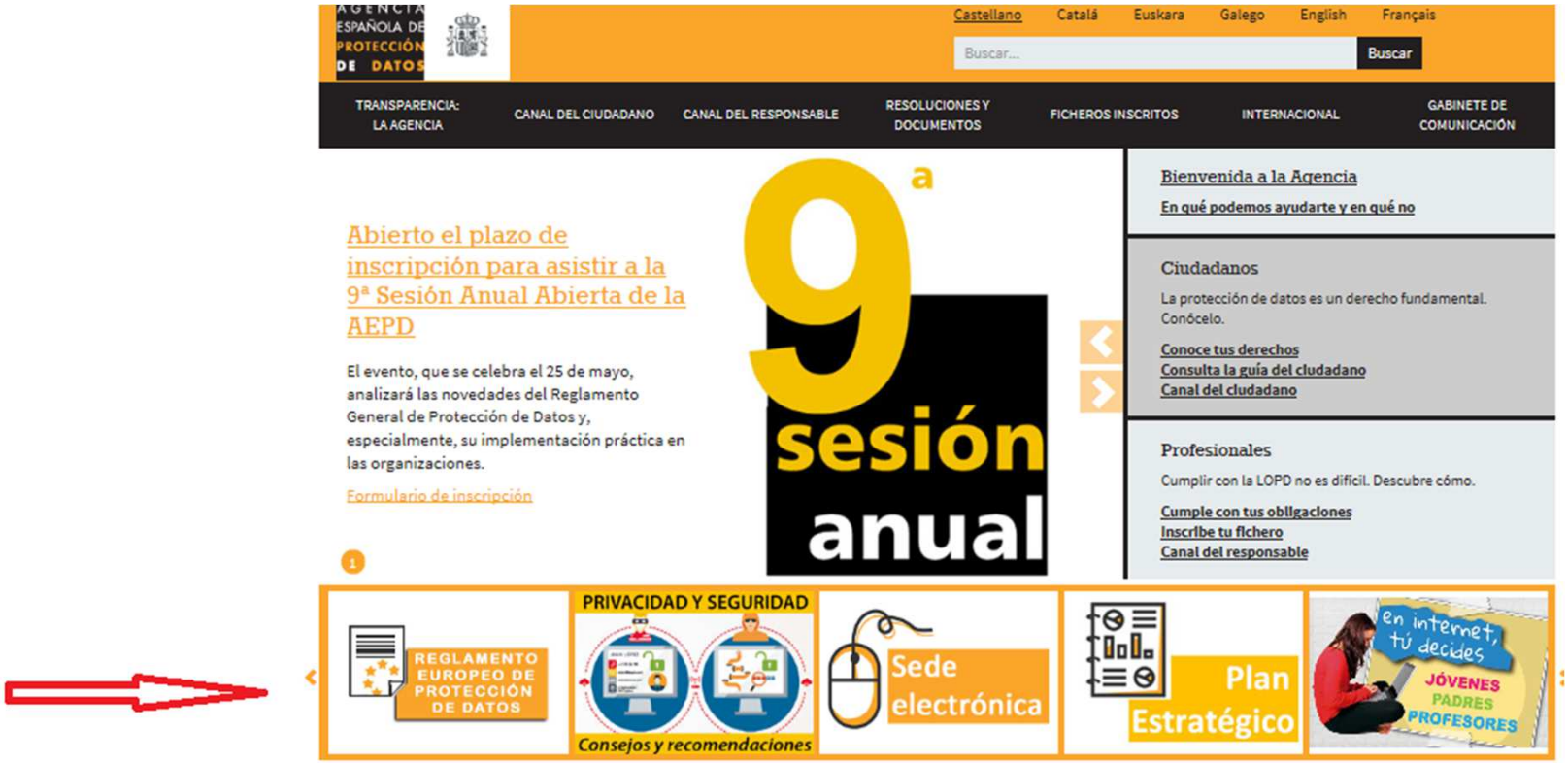
- Sanciones deberán ser efectivas, proporcionadas y disuasorias
- Cantidad deberá modularse atendiendo a circunstancias del caso
- Aplicables a responsables y encargados
- Mecanismo de coherencia sancionador
- Posibilidad de aplicar sanciones penales (Ej. Privación de los beneficios de la infracción)

Sanciones

- Tipificación infracciones y sanciones/apercibimiento:
  - Multa hasta 10 M € o para empresas, optándose por la de mayor cuantía, hasta el 2% de volumen de negocio anual a nivel mundial
    - Obligaciones de responsable o encargado
    - Obligación de organismos de certificación
    - Obligaciones de APD en relación con organismos de supervisión de códigos de conducta
  - Multa hasta 20 M € o hasta el 4%
    - Principios básicos
    - Derechos
    - Transferencias internacionales
  - Multa hasta 20 M € o hasta el 4%
    - Incumplimiento de resoluciones de APD

Información de interés

http://www.agpd.es



Información de interés

- **GUÍAS**
- **ORIENTACIONES**
- **DIRECTRICES SOBRE LA APLICACIÓN**

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es