El nuevo Reglamento Europeo de Protección de Datos

Rafael García Gozalo
Jefe del Departamento Internacional
Agencia Española de Protección de Datos

Armonización

El Reglamento 2016/679 sustituirá a la Directiva 95/46

- Publicado 4 de mayo 2016
- Entrada en vigor a los 20 días de publicación
- 2 años hasta inicio de aplicación

Reglamento implica una máxima armonización

- Aplicación directa, sin necesidad de trasposición
- Desplaza normas nacionales en materias que regula
- Regulación de aplicación o desarrollo sólo posible cuando se prevea expresamente

Armonización

- ¿En qué se pueden diferenciar los EEMM?
  - Definición de conceptos
  - Determinación de condiciones de tratamiento
  - Ejecución de habilitaciones expresas
  - Aplicación judicial
- ¿Cómo se limita la diferenciación?
  - Mecanismos de cooperación y coherencia
  - Control Comisión
  - Decisiones TJUE

Legitimación

Art. 6.1

- *Consentimiento*
- *Ejecución de un contrato*
- *Cumplimiento de una obligación legal*
- *Intereses vitales del interesado o de otra persona física*
- *Misión realizada en interés público o en el ejercicio de poderes públicos*
- *Satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los interés o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones*

Datos especialmente protegidos

- Reglamento mantiene enfoque de la Directiva
  - Lista cerrada de datos "sensibles"
  - Prohibición de tratamiento salvo
    - Consentimiento explícito
    - Listado de excepciones
  - Se requiere base legal para tratar datos en excepciones
- En la lista se incluyen dos nuevos tipos de datos
  - Genéticos (diferenciados de "datos de salud")
  - Datos biométricos dirigidos a identificar unívocamente a una persona física
- Se prevé expresamente que el registro completo de antecedentes penales sólo pueda mantenerse bajo control de poderes públicos

Control por los interesados

- **Consentimiento →**
  - Libre, específico, informado e "inequívoco" → A través de declaraciones o "claras acciones afirmativas"
  - Salvaguardas en articulado y considerandos
    - Situaciones de desequilibrio claro entre interesado y responsable
    - Consentimiento conjunto necesario para varias operaciones
    - Tratamientos vinculados a ejecución de contrato, incluida prestación de servicio, cuando tratamiento no es necesario para esa ejecución o prestación
  - Consentimiento de menores con autorización → 16 años, pudiendo EEMM reducir hasta 13

Transparencia y Derechos

- **Lenguaje** claro e inteligible (en particular, niños)
- Obligación de "facilitar el ejercicio"
- Respuesta → **1 mes** (ampliable 2 meses)
- Formas de ejercicio → Posible vía **electrónica**
- **Gratuidad**, salvo solicitudes "infundadas o excesivas", donde responsables podrá →
  - Exigir un canon
  - Negarse a actuar
- Uso de **iconos** (COM) para proporcionar información

Derechos

- Catálogo tradicional con tres novedades
  - Acceso
  - Rectificación
  - Derecho al borrado y al "olvido"
  - Limitación del tratamiento
  - Portabilidad
  - Oposición

Limitación de tratamiento

- Limitación supone que los datos sólo podrán ser tratados para
  - Conservación
  - Con el consentimiento del interesado
  - Para el ejercicio o defensa de reclamaciones
  - Para proteger los derechos de otra persona física o jurídica
  - Por razones de interés público importante
- Casos en que existe derecho a solicitar la limitación
  - Mientras se verifica de la exactitud de los datos en casos de impugnación por el interesado
  - Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales
  - Cuando el interesado necesite que el responsable conserve los datos para la formulación, el ejercicio o la defensa de reclamaciones
  - Mientras se verifican circunstancias en derecho de oposición

Responsabilidad activa

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

Tipos de medidas

- Mantener "registro de actividades de tratamiento"
- Aplicar medidas de seguridad adecuadas
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Llevar a cabo Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación

Enfoque de riesgo

- Determinadas 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
  - El caso de la notificación de quiebras de seguridad
- Problema de determinación del nivel de riesgo
- Nuevo enfoque de supervisión → Más fluidez en el análisis

Protección de Datos desde el diseño

- **Medidas técnicas y organizativas adecuadas** (p.ej. seudonimización, minimización) para aplicar principios de PD de forma eficaz y proteger los derechos
- **En el momento de determinar los medios para el tratamiento y en el momento del tratamiento** (integrar necesarias garantías)
- 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

Protección de Datos por defecto

- 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 DPO
  - Fines
  - Descripción de categorías de interesados y datos personales
  - Categorías de destinatarios existentes o previstos (inclusive en terceros países u organizaciones internacionales)
  - TID a terceros países u organizaciones internacionales y documentación de garantías para TID exceptuadas sobre base de intereses legítimos imperiosos
  - Cuando sea posible, plazos previstos para supresión de datos
  - Cuando sea posible, descripción general de medidas de seguridad

Medidas de seguridad

- 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

- La adhesión a un **código de conducta o a un mecanismo de certificación** podrá servir de elemento para demostrar el cumplimiento de los requisitos de seguridad

Notificación de violaciones de seguridad de los datos

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 de los datos

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

- Deberá realizarse cuando sea probable que el tratamiento previstos presente un alto riesgo específicos 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 o que les afecten significativamente de modo similar;
  - tratamiento a gran escala de las categorías especiales de datos
  - 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

Evaluación de impacto

- Consulta a APD cuando una EIPD muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo → Considerando 94 *"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 obligar a los responsables a consultar a la autoridad de control y a recabar su autorización previa 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
  - las actividades principales de responsable o encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
  - las actividades principales de responsable o encargado 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

- Nombramiento basado en →
  - Cualidades profesionales
  - Conocimientos especializados del Derecho y la práctica en materia de protección de datos
  - Capacidad para desempeñar sus funciones
- Relación laboral o mediante contrato de servicios
- Podrá desempeñar otras funciones, si no hay conflicto de intereses
- No podrá recibir ninguna instrucción en lo que respecta al desempeño de dichas 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 de la Unión o de los EEMM
- **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
- Regulación más detallada que en Directiva → Contrato que fije
  - 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…

Transferencias internacionales

- El Reglamento parte del criterio clásico de que los datos de los europeos sólo pueden enviarse a países que ofrezcan un nivel adecuado de protección
- Se amplían y flexibilizan instrumentos de garantía
  - Responsables y encargados pueden ser exportadores
  - Instrumentos jurídicamente vinculantes y ejecutables entre autoridades u organismos públicos
  - 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, junto con compromisos vinculantes y ejecutables del responsable o encargado en el tercer país para aplicar las salvaguardas apropiadas, incluidos los derechos del interesado
- Ampliación de excepciones para casos basados en interés legítimo del responsable

Supervisión

- **Aspectos positivos →**

  Potestad sancionadora armonizada para APD

- **Insuficiente claridad y precisión →**
  - **Definición de infracciones**
  - **Cuantía de sanciones**
  - **Naturaleza de las medidas alternativas o acumulativas a las económicas (apercibimientos, amonestaciones,…)**
  - **Prescripción**

- **Positiva la posibilidad de adecuar sanciones al tamaño de la empresa, pero →**
  - **Dudas sobre criterios para fijar límites máximos**
  - **Dudas sobre clasificación de infracciones**

Supervisión

Acciones correctivas →

- **Advertencia** cuando las operaciones de tratamiento previstas puedan infringir RGPD
- **Apercibimiento** cuando las operaciones de tratamiento hayan infringido RGPD
- Ordenar que se **atiendan las solicitudes** de ejercicio de los derechos
- Ordenar que las **operaciones de tratamiento se ajusten a las disposiciones del RGPD**
- Ordenar al responsable que **comunique al interesado las violaciones de la seguridad** de los datos personales
- Imponer una **limitación temporal o definitiva del tratamiento**, incluida su prohibición

Supervisión

- Cantidad deberá modularse atendiendo a circunstancias del caso
- Aplicables a responsables y encargados
- Esquema básico de infracciones y sanciones
  - 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 organismos de supervisión de códigos de conducta
  - Multa hasta 20 M € o hasta el 4%
    - Principios básicos
    - Derechos
    - Transferencias internacionales..
    - Incumplimiento de resoluciones de APD

¡MUCHAS GRACIAS!