El nuevo Reglamento Europeo de Protección de Datos

Jesús Rubí Navarrete
Adjunto a la Directora
Agencia Española de Protección de Datos
Santiago de Chile
Septiembre 2016

Armonización

Un Reglamento 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

Contenido

- **Texto largo y detallado → 99 artículos y 173 considerandos**
- **11 Capítulos →**
  - Disposiciones Generales
  - Principios
  - Derechos de los interesados
  - Responsable y encargado
  - Transferencias internacionales
  - Autoridades de control independientes
  - Cooperación y coherencia
  - Recursos, responsabilidad y sanciones
  - Disposiciones sobre situaciones específicas de tratamiento
  - Actos delegados y actos de ejecución
  - Disposiciones finales

Ámbito material de aplicación

Artículo 2

" 1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión

b) por parte de las instituciones, órganos u organismos de la Unión

c) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del TUE

d) por parte de una persona física sin interés lucrativo en el ejercicio de actividades exclusivamente personales o domésticas

e) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales o de protección y prevención frente a las amenazas a la seguridad pública."

Ámbito territorial de aplicación

Artículo 3

*"1. El presente Reglamento se aplica al tratamiento de datos personales en el **contexto de las actividades** de un **establecimiento del responsable o del encargado** del tratamiento **en la Unión**.*

*2. El presente Reglamento se aplica al tratamiento de datos personales de **interesados que residan en la Unión** por parte de un **responsable o encargado** **no establecido en la Unión**, cuando las actividades de tratamiento estén relacionadas con:*

*a) la **oferta de bienes o servicios** a dichos interesados en la Unión, independientemente de si a estos se les requiere un pago*

*b) el **control de su comportamiento,** en la medida en que este tenga lugar en la Unión*

Principios

Principios se mantienen similares a Directiva, con refuerzo en algunos matices

- Licitud, lealtad y transparencia
- Limitación de finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

Legitimación

Art. 6.1

a) consentimiento para el tratamiento de sus datos personales para uno o más fines específicos;

b) ejecución de un contrato en el que el interesado es parte o para la aplicación, a petición de éste, de medidas precontractuales;

c) cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento,

d) intereses vitales del interesado o de otra persona física;

e) cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la 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.

Control de 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

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 sólo pueda mantenerse bajo control de poderes públicos

Derechos

- Catálogo tradicional con tres novedades
  - Información
  - Acceso
  - Rectificación
  - Derecho al borrado y al olvido
  - Limitación del tratamiento
  - Portabilidad
  - Oposición
- Previsiones sobre ejercicio de estos derechos
  - Lenguaje claro e inteligible
  - Obligación de "facilitar el ejercicio"
  - Plazos de respuesta → 1 mes
  - Formas de ejercicio → Posible vía electrónica
  - Gratuidad
  - Uso de iconos para proporcionar información

Derecho al olvido y al borrado

- **Derecho de supresión (Derecho al olvido) (art. 17)**
  - **Obligación del responsable de informar a terceros responsables de la solicitud del interesado de supresión de enlaces, copias o réplicas**
    - **Adopción de medidas por el responsable**
    - **Tecnología disponible y coste**
    - **Medios a su disposición**
    - **Salvo imposibilidad o esfuerzo desproporcionado**
  - **Excepciones**
    - **Libertad de información y expresión (entre otras)**

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**

Portabilidad

- *"El interesado tendrá **derecho a recibir los datos personales que le incumban**, que haya facilitado a un responsable del tratamiento, **en un formato estructurado, de uso común y lectura mecánica**, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:*
  - *a) el tratamiento esté basado en el **consentimiento** o en un **contrato** y*
  - *b) el tratamiento se efectúe por **medios automatizados**"*

- **Transmisión directa de responsable a responsable condicionada a que sea *"técnicamente posible"***

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 de "cumplir" dirigidas a evitar o paliar incumplimientos

- La no aplicación de estas medidas es sancionable

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
- 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

- 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

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
- 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 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 a interesados

- Cuando es probable que la quiebra entrañe alto riesgo para los derechos y libertades de interesados
- Sin dilación indebida
- También se prevé contenido mínimo, que no incluye posibles medidas paliativas
- Excepciones
  - Implementación de medidas de protección tecnológica adecuada a los datos afectados, a satisfacción de la APD, 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 los derechos y libertades del interesado
- APD puede obligar a notificar a interesados
- Competencia Rgto/LGT

Evaluación de impacto

- Deberá realizarse cuando sea probable que los tratamientos 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
  - Deban ser autorizados por APD según el Reglamento
- 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 la opinión de los interesados

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, que deberán evaluarse, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados
  - 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
- Publicación de "datos de contacto" y comunicación a 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

Relaciones Responsable – Encargado

Algunas peculiaridades:

- Previsión de que el responsable "realice **auditorías** y 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
- Obligación de **informar** al responsable "si, en su opinión, una **instrucción infringe el presente Reglamento** o las disposiciones nacionales o de la Unión en materia de protección de datos"
- Posibilidad de **"contratos modelo"**

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

Transferencias internacionales

- **Ampliación de excepciones**
  - Casos basados en interés legítimo imperioso del responsable o del encargado prevalente sobre los derechos o intereses del interesado
  - No repetitivas
  - Afecta a un número limitado de interesados
  - Evaluación de las circunstancias concurrentes y ofrecimiento de garantías adecuadas para la protección de los datos

Modelo de supervisión

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

Modelo de supervisión

¿Qué se considera sanción?

- Multas económicas lo son →
  - Han de ser proporcionadas, disuasorias y efectivas
  - Hay criterios de modulación
  - Se asocian con incumplimientos específicos
- ¿Otras "acciones correctivas"? →
  - Se aplican junto a o en lugar de multas
  - No parecen afectadas por criterios de modulación
  - Listado mezcla acciones típicamente sancionadoras con otras de naturaleza mas discutible
- Pero →
  - Reglamento alude en considerandos a que contiene "multas y otras sanciones administrativas"
  - EEMM obligados a establecer sanciones adicionales, administrativas o penales, especialmente cuando Reglamento no prevé multas administrativas

Modelo de supervisión

- Sanciones deberán ser efectivas, proporcionadas y disuasorias
- Cantidad deberá modularse atendiendo a circunstancias del caso
- Aplicables a responsables y encargados
- Tipificación infracciones y sanciones:
  - Multa hasta 10 M € o para empresas, optándose por la demayor 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

¡MUCHAS GRACIAS!