Visión de la Agencia Española de Protección de Datos sobre el nuevo Reglamento Europeo de Protección de Datos

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

Armonización

Instrumento elegido

- **Reglamento implica una máxima armonización**
- **Tal como fue propuesto contiene márgenes de flexibilidad**
- **Cambios para "sector público" pueden abrir espacios de dispersión →**

> ***"6.2 bis. Los Estados miembros podrán mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento de datos personales para el cumplimiento de lo dispuesto en el artículo 6, apartado 1, letras c) y e), determinando con más precisión los requisitos específicos para el tratamiento y otras medidas para garantizar un tratamiento lícito y equitativo, también para otros casos específicos de tratamiento, tal y como prevé el capítulo IX."***

Ambito de aplicación

- **Delimitación de los ámbitos respectivos de Reglamento y Directiva →**

  "…fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, de ejecución de sanciones penales o de protección y prevención frente a las amenazas a la seguridad pública"

- **Aplicabilidad a responsables y encargados no establecidos en la UE siempre que realicen tratamientos derivados**
  - **de una oferta de bienes o servicios (incluidos sin contraprestación económica) a interesados en la Unión o**
  - **de un seguimiento de su actividad**

Bases legales

- Texto final mantiene a grandes rasgos enfoque actual
- Se amplía **catálogo de finalidades compatibles** para tratamientos sucesivos
- Dudoso alcance de referencia a que para tratamientos sucesivos para **fines compatibles** "*no se exigirá una base jurídica aparte, distinta de la que permitió la obtención de los datos*"
- Criterios de **determinación de compatibilidad**
- Confusa **descripción del principio de no tratamiento para finalidades incompatibles**

Control de los interesados

- **Definición del consentimiento →**
  - Se mantiene su carácter **"inequívoco"**
  - Ese carácter se debe plasmar en **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
- **Información**
- **"Derecho al olvido" y a la portabilidad**
- **Redefinición del 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 de "cumplir" dirigidas a evitar o paliar infracciones

- La no existencia de estas medidas es sancionable

Responsabilidad activa

Tipos de medidas

- Mantener documentación
- 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

Enfoque de riesgo

¿Cómo medir riesgo y cómo guiar a responsables?

Considerando 60 "Debe quedar establecida la responsabilidad del responsable en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe (…) estar obligado a aplicar las medidas oportunas y poder demostrar la conformidad de (…) las actividades de tratamiento con lo dispuesto en el presente Reglamento (...). Estas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

Enfoque de riesgo

¿Cómo medir riesgo y cómo guiar a responsables?

Considerando 60bis "Dichos riesgos, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños físicos o morales, en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, perjuicio para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, cambio no autorizado de la seudonimización o cualquier otro perjuicio económico o social significativo; o en los casos en los que se prive a los interesados de sus derechos y libertades o de ejercer el control sobre sus datos personales; cuando los datos personales tratados revelen el origen étnico o racial, (lista de datos sensibles); cuando se evalúen aspectos personales, (…), con el fin de crear o utilizar perfiles personales; cuando se traten datos personales de personas vulnerables, en particular niños; cuando el tratamiento implique una gran cantidad de datos personales y afecte a una gran cantidad de interesados."

Considerando 60ter "La probabilidad y la gravedad del riesgo deberá evaluarse en función de la naturaleza, ámbito, contexto y fines del tratamiento de datos. El riesgo deberá estimarse por medio de una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo elevado. (Un riesgo elevado es un riesgo particular de perjuicio a los derechos y libertades de las personas físicas)"

Enfoque de riesgo

¿Cómo medir riesgo y cómo guiar a responsables?

- El Consejo Europeo de Protección de Datos también puede publicar directrices sobre operaciones de tratamiento de las que se considera que es poco probable que den lugar a un riesgo elevado para los derechos y libertades de las personas físicas e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión

- Códigos de conducta (…), certificaciones (…), orientaciones del Consejo Europeo de Protección de Datos o indicaciones proporcionadas por un DPD podrían proporcionar directrices para la aplicación de medidas apropiadas y para demostrar el cumplimiento por parte del responsable o el encargado del tratamiento, especialmente en lo referido a la identificación del riesgo relacionado con el tratamiento, la evaluación del mismo en términos de origen, naturaleza, probabilidad y gravedad, y la identificación de buenas prácticas para mitigar el riesgo.

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
  - 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

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

¡MUCHAS GRACIAS!