8º foro sobre el SISTEMA DE INFORMACIÓN del Sistema Nacional de Salud

18/octubre/2017

Ministerio de Sanidad, Servicios Sociales e Igualdad
Salón de Actos Ernest Lluch

"El Sistema de Información del Sistema Nacional de Salud en el siglo XXI"

# IMPACTO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN LOS SERVICIOS PÚBLICOS DE SALUD

Jesús Rubí Navarrete
Adjunto a la Directora
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: 25 de mayo de 2018

# Principios

Principios se mantienen similares a Directiva, con refuerzo en alguno de ellos

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

# El deber de informar/principio de transparencia en el Reglamento

Se incrementa la información que habrá de facilitarse cuando los datos se recaban del afectado

- Identidad y los datos de contacto del responsable y, en su caso, de su representante
- Datos de contacto del delegado de protección de datos
- Fines y base jurídica del tratamiento
- Intereses legítimos del responsable o de un tercero
- Destinatarios o las categorías de destinatarios de los datos personales
- Transferencias previstas

# El deber de informar/principio de transparencia en el Reglamento

- Plazo de conservación
- Derechos de acceso, rectificación o supresión, limitación del tratamiento, oposición y portabilidad
- Posibilidad de revocación del consentimiento
- Derecho a presentar una reclamación ante una autoridad de control;
- Si la comunicación de datos personales es obligatoria y las posibles consecuencias de que no facilitar los datos

# El deber de informar/principio de transparencia en el Reglamento

- Existencia de decisiones automatizadas, incluida la elaboración de perfiles la lógica aplicada y las consecuencias previstas

Si los datos no se recaban del interesado deberá además informársele de:

- Categorías de datos que se van a tratar
- Fuente de la que proceden los datos personales y, en su caso, si proceden de "fuentes de acceso público"
- AEPD: Información por capas y tablas

# 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

# 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
- Problema de determinación del nivel de riesgo

# PDdD

## 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

# PDdD

## 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 contacto de responsable, corresponsable, representante y DPO
  - Fines
  - Descripción de categorías de interesados y datos personales

# Registro de tratamientos

- 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
- También se prevé 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 los derechos y libertades del interesado
- 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

# 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 el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales

# DPD

- Nombramiento basado en →
  - Cualidades profesionales (Certificación)
  - 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

# DPD

- 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
- No responsabilidad personal por incumplimientos

# Responsable y encargado del tratamiento

- 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

# Responsable y encargado del tratamiento

- Confidencialidad de personas que manejen datos
- Medidas de seguridad
- 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 ( seguridad, notificación de violaciones de seguridad, evaluaciones de impacto, consulta previa a la AEPD)

# ¡MUCHAS GRACIAS!