Impacto del Reglamento General de Protección de Datos en la Consejería de Sanidad de la Comunidad de Madrid (CSCM)

Madrid, 12 de abril de 2018

SaludMadrid

Servicio Madrileño de Salud
Dirección General de Sistemas de Información Sanitaria

Comunidad de Madrid

ÍNDICE

1. RGPD: Qué es y objetivos

El Reglamento General de Protección de Datos: legislación europea que regula la protección de las personas físicas en relación con el tratamiento de sus datos personales.

Objetivos:

REGLAMENTO EUROPEO
DE PROTECCIÓN DE DATOS

- **Fortalecer el derecho a la privacidad, especialmente *on line*.**
- **Crear una normativa eficaz y uniforme.**
- **Facilitar el flujo internacional de datos, asegurando una adecuada protección de los mismos.**

2. Marco normativo

NUEVO Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento General de Protección de Datos (RGPD).

- Directamente aplicable en el Espacio Económico Europeo (EEE)* a partir del 25/05/2018.
- Art. 18.4 Constitución Española (CE).
- Ley Orgánica 15/1999, de Protección de Datos de carácter Personal (LOPD).
- Real Decreto 1720/2007, Reglamento de desarrollo de la LOPD (RLOPD).

Nueva LOPD

NORMATIVA SECTORIAL:

- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 41/2002 de Autonomía del Paciente (LAP).
- Orden 491/2013, de la Consejería de Sanidad, Política de seguridad de la información, Consejería de Sanidad de la Comunidad de Madrid.
- Normativa vigente en materia de investigación, ensayos clínicos y docencia.

*UE + Islandia + Liechtenstein + Noruega.

3. Impacto del RGPD en la CSCM

APLICABILIDAD DEL REGLAMENTO EN ADMINISTRACIONES PÚBLICAS

- ✓ESPECIFICACIONES PROPIAS PARA EL SECTOR PÚBLICO.
- ✓INTERRELACIÓN CON NORMATIVA ESPECÍFICA DEL SECTOR SANITARIO.

FECHA LÍMITE:
25 MAYO 2018

- ✓NECESIDAD DE REALIZAR MODIFICACIONES PARA LA ALINEACIÓN DE LA NORMATIVA Y LA PRÁCTICA DE LA CSCM.
- ✓LA AEPD CATALOGA EL IMPACTO EN AAPP EN ACCIONES ESPECÍFICAS.

3. Impacto en la CSCM

1. REGISTRO DE ACTIVIDADES DE TRATAMIENTO.

- Sustituye necesidad de notificar ficheros a la AEPD.
- Debe mantenerse actualizado a disposición de las autoridades.
- Se comunicarán a la OSSI los diferentes tratamientos realizados para su registro y publicidad.

2. NECESIDAD DE IDENTIFICAR FINALIDADES Y BASE JURÍDICA DEL TRATAMIENTO.

- Debe recogerse en registro de actividades de tratamiento.
- Datos especialmente sensibles, regla general de prohibición de uso, excepciones para tratamientos necesarios (art. 9.2 RGPD):
  - Fines de prevención, asistencia sanitaria o salud pública.
  - Para interés público esencial.
  - Servicios asistencia social.
  - En los casos que establezca la legislación española (normativa sectorial).

3. Impacto en la CSCM

3. TRATAMIENTO CON FINES DE INTERÉS PÚBLICO O EJERCICIO DE PODERES PÚBLICOS.

- Necesidad de existencia de regulación con rango legal como legitimación de tratamiento (normativa sectorial): Ley General de Sanidad, Ley de autonomía del paciente, Ley de salud pública.

4. CONSENTIMIENTO COMO BASE JURÍDICA PARA EL TRATAMIENTO.

- Para actividades no relacionadas con asistencia sanitaria o interés público (investigación clínica y docencia, entre otros). Debe cumplir los siguientes requisitos:
  - Ser informado, libre y específico.
  - Otorgado mediante manifestación claramente afirmativa.
  - Se prohíbe el consentimiento tácito (basado en inacción), incluso para tratamientos iniciados con anterioridad.

5. DERECHO DE INFORMACIÓN.

- Ampliación de deber de información, necesidad de catalogar y adecuar los clausulados existentes.
- La información debe ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.
- Posibilidad de información por capas (servicios electrónicos y cartelería).

3. Impacto en la CSCM

6. EJERCICIO DE DERECHOS.

- Establecimiento de mecanismos visibles, accesibles y sencillos, incluidos medios electrónicos.
- Procedimientos para verificar la identidad de los interesados.
- Respuesta en plazo (30 días), colaboración de encargados del tratamiento (debe constar en contrato).

7. ENCARGADO DE TRATAMIENTO.

- Diligencia debida: valorar si los encargados de tratamiento ofrecen garantías de cumplimiento del RGPD.
- Ampliación del contenido de contratos, necesidad de catalogar y adecuar los contratos y convenios existentes:
  - Encargado de tratamiento.
  - Encargado de tratamiento mutuo.
  - Encargado de tratamiento sin acceso a datos.
  - Cesiones o comunicaciones de datos.

8. ANÁLISIS DE RIESGOS.

- Necesidad de realizar análisis de riesgos de los tratamientos de datos.
- El resultado del análisis de riesgos determina medidas de seguridad a aplicar.
- En AAPP las medidas de seguridad las dicta el Esquema Nacional de Seguridad.

3. Impacto en la CSCM

9. EVALUACIÓN DE IMPACTO.

- Para los tratamientos que conlleven un riesgo alto.
- Requiere elaborar informe sobre la base jurídica del tratamiento y las medidas a implicar para mitigar el riesgo.

10. DESIGNACIÓN DELEGADO DE PROTECCIÓN DE DATOS (DPD).

- Las AAPP están obligadas a nombrar un DPD, con requisitos de cualificación y competencia.
- En la CSCM, revestirá la forma de Organismo Colegiado denominado Comité DPD.
- Su nombramiento se debe comunicar a la AEPD.
- Se deben establecer mecanismos para que los interesados puedan contactar con el DPD.

11. DETECCIÓN Y NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD.

- Establecimiento de mecanismos para la detección y evaluación del riesgo de la violación de seguridad.
- Establecimiento de protocolo de comunicación previa al Delegado de Protección de Datos (DPD) de la CSCM.
- Se deben notificar a la AEPD y si les afecta directamente, a los interesados.
- Registro y seguimiento de cualquier incidente de seguridad.

12. TRANSFERENCIAS INTERNACIONALES DE DATOS.

- Se amplía catálogo de instrumentos con garantías suficientes, que no requieren autorización de la AEPD.

5. Plan de Acción

REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

SITUACIÓN ACTUAL.

FASE 1.

FINALIZADA.

- Análisis de situación e impacto.
- Identificación actividades de tratamiento.
- Identificación de roles y responsabilidades.
- Propuesta Comité DPD.

FASE 2.

EN DESARROLLO.

- Catalogación de clausulados a modificar.
- Elaboración de modelos:
  - Cláusulas informativas.
  - Cartelería.
  - Encargados de tratamiento.
  - Convenios.
- Modificación de informes y protocolos afectados.
- Estudio y adaptación metodología Magerit para análisis de riesgos.
- Tríptico plan de comunicación a Gerentes.
- Formación y concienciación a Hospitales.

FASE 3.

PRÓXIMOS PASOS.

- Aprobación del Plan de Acción en Comité SERMAS
- Publicaciones oficiales BOCM.
- Difusión de documentación e instrucciones para su implementación desde el CDPD.

Muchas gracias

SaludMadrid