EL REGLAMENTO GENERAL DE PROTECCION DE DATOS

“Enfoque preventivo”

23 abril 2018
M. Rosario Heras Carrasco
Unidad de Evaluación y Estudios Tecnológicos
Agencia Española de Protección de Datos

LEGISLACION ACTUAL (LOPD)

- Falta claridad en los objetivos que la norma pretende conseguir: busca proteger datos personales pero no se identifica frente a qué o en qué medida.
- Orientada a procesos, se establece lo que hay que hacer pero no por qué, para evitar qué daño o para mejorar qué aspecto de la protección.
- Son obligaciones genéricas aplicables a todos los responsables sin reconocer diversidad o contexto.
- Obligaciones no priorizadas más allá de que pueda deducirse de posibles esquemas sancionatorios.

32 DIAS hasta 25/5/2018

REGLAMENTO GENERAL DE PROTECCION DE DATOS

- Publicado en abril de 2016, de plena aplicación el 25 de mayo de 2018. NO HAY MORATORIA

- Reglamento implica máxima armonización

  - Aplicación directa, sin necesidad de normas internas de trasposición
  - Desplaza normas nacionales
  - Regulación adicional sólo posible cuando se prevea expresamente

Responsabilidad activa

- Los responsables del **tratamiento** aplicarán:

  - Medidas técnicas y organizativas apropiadas para **garantizar** y estar en condiciones de **demostrar** el cumplimiento
  - Teniendo en cuenta la naturaleza, el ámbito, contexto y fines del tratamiento así como los riesgos de probabilidad y gravedad para los derechos y libertades

- Medidas revisables y se actualizarán cuando sea necesario
- Se considera insuficiente "no incumplir". **Demostrar que cumplo**
- Incluye medidas preventivas para evitar el incumplimiento, **no para cumplir**

Tipos de medidas

MEDIDAS

- Mantener **registro** de actividades de tratamiento
- Protección de Datos desde el **Diseño** y por **Defecto**
- Aplicar **medidas de seguridad adecuadas al riesgo**
- Realizar una **evaluación de impacto**
- Autorización previa o **consulta previa** con la APD
- Designación **Delegado de Protección de Datos** (DPO)
- Notificación de **violaciones** de seguridad
- Adopción **Códigos de conducta** y esquemas de **certificación**

Registro de actividades de tratamiento

- Desaparece el concepto de fichero asociado a inscripción
- Desaparece la obligación de notificar los ficheros a la LOPD
- No debe notificarse a la AEPD, lo tiene que conservar el responsable o encargado
- Se aplica a responsable y encargado del tratamiento
- Debe elaborarlo el responsable o su representante
- Debe constar por escrito

ES LA PARTE MAS IMPORTANTE SOBRE LA QUE GESTIONAR EL RESTO DE MEDIDAS

Registro de actividades de tratamiento

Contenido:

- Nombre y datos de contacto del responsable y DPD
- Fines
- Descripción de categorías de interesado y datos personales
- Categorías de destinatarios (internacionales tb)
- Transferencias de datos
- Plazos de supresión (cuando sea posible)
- Descripción general de medidas técnicas y organizativas de seguridad (cuando sea posible) OJO AAPP transparencia

Base jurídica del tratamiento

Desde el diseño y por defecto

Art. 25 RGPD

El responsable del tratamiento aplicará medidas técnicas y organizativas como la seudonimización:

- En el momento de determinar los medios de tratamiento o en el momento del propio tratamiento
- Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, el ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas
- Minimización de datos

¿para qué?

Para cumplir con los requisitos del RGPD y proteger los derechos de los interesados

Medidas de seguridad adecuadas al riesgo

- Desaparece niveles de seguridad y detalle de medidas concretas
- Aparece la aplicación de medidas adecuadas en función del **riesgo para derechos y libertades** de las personas físicas
- El riesgo **no es sólo medidas de seguridad**
- Riesgos que presente el tratamiento de datos como consecuencia de destrucción, pérdida o alteración
- Medidas a incluir:
  - seudonimización y cifrado
  - capacidad de restaurar la confidencialidad, integridad, disponibilidad y resiliencia de sistemas y servicios de tratamiento
  - capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida ante incidente técnico o físico
  - proceso de verificación, evaluación y valoración de la eficacia de las medidas

Medidas de seguridad adecuadas al riesgo

Los riesgos para los derechos y libertades de las personas físicas pueden deberse a que el tratamiento de datos pudiera provocar **daños y perjuicios físicos, materiales o inmateriales.**

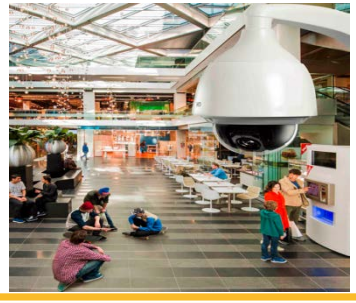
¿Cuándo? Si el tratamiento puede dar lugar a:

- problemas de discriminación
- usurpación de identidad o fraude
- pérdida financiera
- daños para la reputación
- perdida de confidencialidad de datos sujetos al secreto profesional
- reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo

Evaluaciones de impacto

¿Cuándo hay que hacer una evaluación de impacto?

- Cuando sea probable que el tratamiento previsto presente un **alto riesgo**, en particular si utiliza nuevas tecnologías
- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas basada en un tratamiento automatizado, como **elaboración de perfiles** y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas
- Tratamiento a **gran escala de datos personales** que revelen origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, biométricos, datos relativos a la salud, vida sexual u orientación sexual, además datos personales relativos a condenas e infracciones penales
- **Observación sistemática** a gran escala de una zona de acceso público con dispositivos optométricos



Evaluaciones de impacto

Alto Riesgo

- Si se priva a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales
- Cuando los datos personales revelen el origen étnico o racial, opiniones políticas, religión o creencias filosóficas, militancia en sindicatos
- Tratamiento de datos genéticos, salud, vida sexual o condenas e infracciones penales
- Si se evalúen aspectos personales (análisis y predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, comportamiento, situación o movimientos con el fin de crear perfiles personales)
- Tratamientos de datos personales de niños

Evaluaciones de impacto

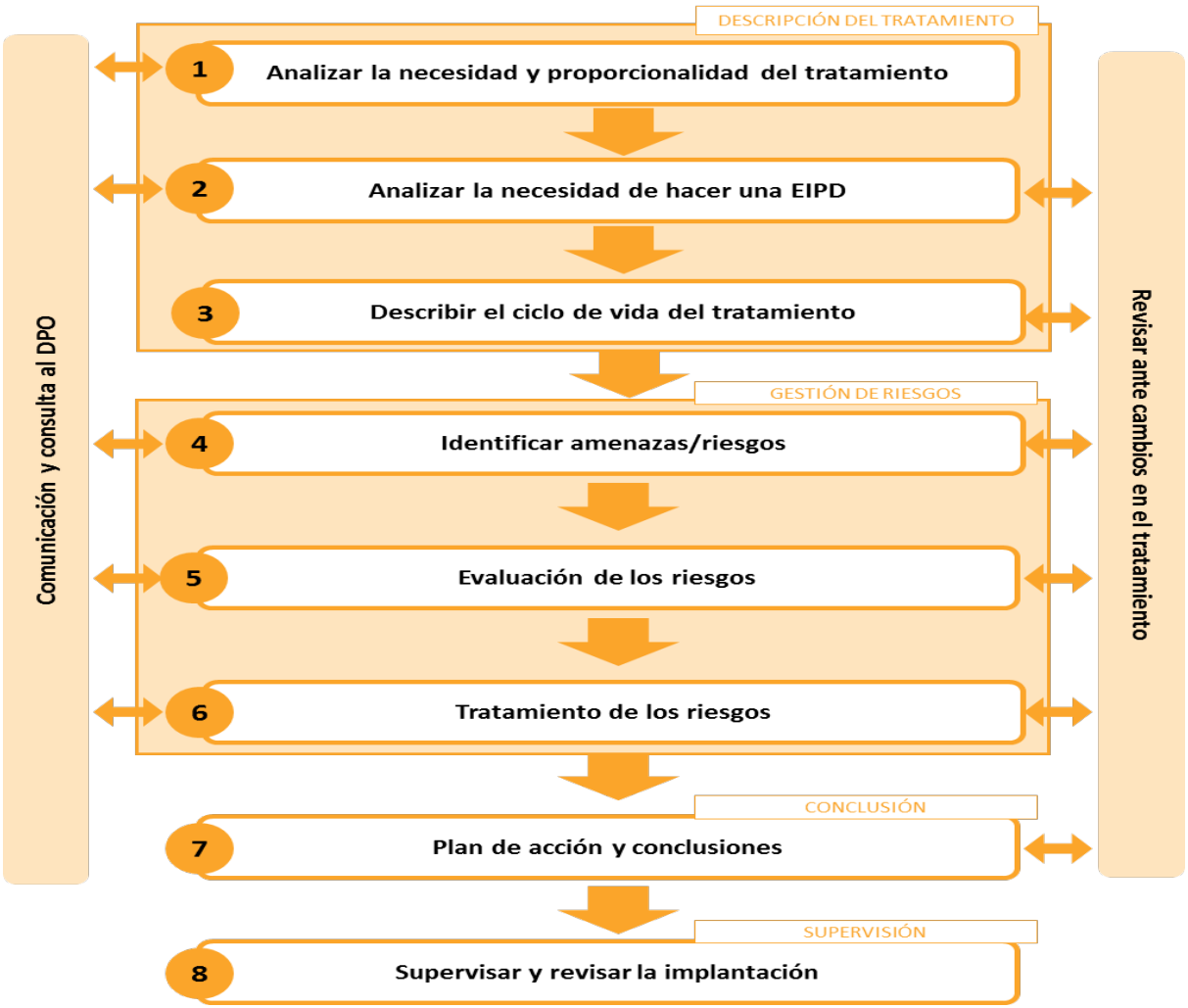
Gran Escala (WP29)

- El número de interesados involucrados, bien como cifra concreta o como proporción de la población correspondiente
- El volumen de datos o el abanico de diferentes conceptos de datos que se procesan
- La duración, o permanencia, de la actividad de tratamiento de datos
- El alcance geográfico de la actividad de tratamiento

¿Qué es una evaluación de impacto?

- Debe realizarse con **anterioridad** a la implantación de un nuevo producto o servicio o sistema de información.
- No es una mera comprobación del cumplimiento normativo.
- **Proceso sistemático** para evaluar los riesgos existentes para la privacidad de las personas y su nivel de impacto.
- Permite **analizar y gestionar** los riesgos identificados que un determinado sistema de información, producto o servicio puede entrañar y adoptar las medidas necesarias para eliminarlos o mitigarlos.
- Debe ser **sistemática** y **reproducible**.
- Orientada a **procesos** más que a generar un informe final.
- Debe permitir **identificar** de forma clara a los **responsables** de las distintas tareas.

Évaluación de impacto



FASES

Descripción del Tratamiento

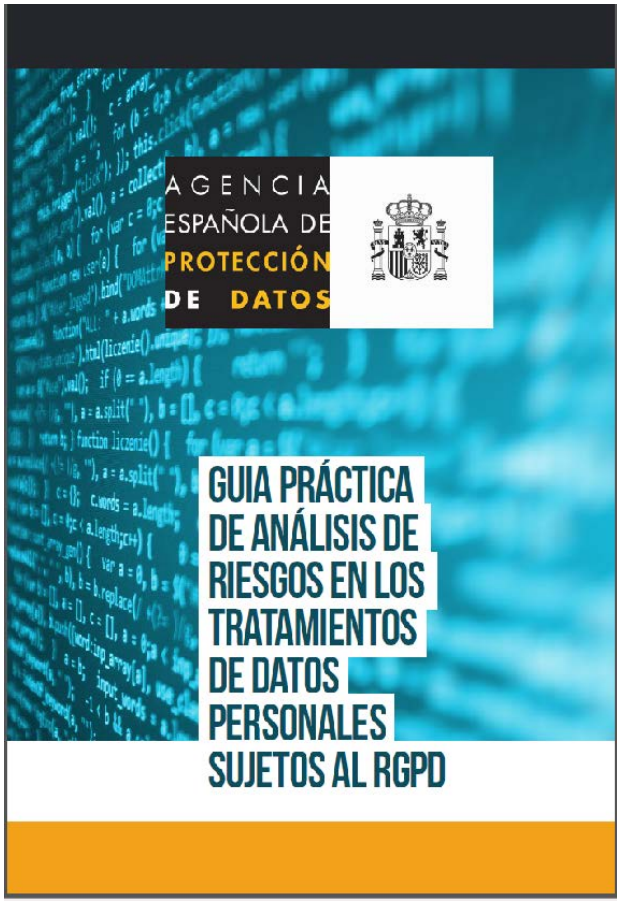
Gestión de riesgo

Conclusión

Supervisión

Evaluaciones de impacto

Evaluaciones de impacto



www.agpd.es

Consulta Previa AEPD

- Cuando una evaluación de impacto muestre que si se inicia el tratamiento, éste entrañaría un **alto riesgo** si el responsable no toma medidas para mitigarlo **y**
- **si el responsable del tratamiento considera que el riesgo no puede mitigarlo por medios razonables teniendo en cuenta la tecnología disponible y costes de aplicación**

La APD considera que el tratamiento objeto de la consulta podría infringir el Reglamento:

- Asesorar por escrito al responsable /encargado. Plazo de 8 semanas desde la solicitud
- Utilizar cualquiera de sus poderes recogidos en el artículo 58, (ampliar información, investigar, incluido prohibir el tratamiento)

DPO

- Obligatorio:
  - AAPP
  - Responsables o encargados que tengan entre sus actividades principales tratamientos que requieran una observación habitual y sistemática de interesados a gran escala o traten datos a gran escala
- En el proyecto de LOPD se recoge que responsables deben nombrar DPD y entre ellos constan:

  "Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en material de información y documentación clínica"

DPO

- En las Administraciones Públicas puede nombrarse un solo DPD para varias entidades
- Nombrado atendiendo a cualificaciones profesionales y formación en materia de protección de datos
- Designación pública y comunicada a la AEPD
- No tiene que estar certificado
- Autonomía de funciones y su relación a nivel superior
- Actuará como punto de contacto para los interesados
- El responsable facilitará todos los recursos que necesite.
- Puede ser un miembro del personal del responsable del tratamiento o del encargado del tratamiento (DPD interno) o «cumplir las tareas sobre la base de un contrato de servicios». Puede ejercerse sobre la base de un contrato de servicios celebrado con un individuo u organización

Funciones

- Informar y asesorar a responsable y encargado, documentando esa actividad
- Supervisar la puesta en práctica de las políticas de protección de datos, incluidas la formación y la auditoría
- Supervisar la aplicación del Reglamento en lo relativo a PbD, PbDef y derechos de los interesados
- Asegurar la existencia y mantenimiento de documentación obligatoria
- Supervisar gestión de quiebras de seguridad
- Supervisar la realización de Evaluaciones de Impacto y la solicitud de consultas que se requieran
- Cooperar con la APD en el marco de sus tareas
- Actuar como punto de contacto para la APD y los interesados
- Información directa a la dirección
- NO SON RESPONSABLES DEL INCUMPLIMIENTO DEL RGPD

Violaciones de seguridad

- Incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma o la comunicación o acceso no autorizado a dichos datos.
- Comunicada a la AEPD a menos que sea improbable que suponga un riesgo para los derechos y libertades
- Plazo de 72 horas desde que tiene constancia
- Contenido mínimo: naturaleza, categorías de datos y de interesados, medidas adoptadas para solventarla, medidas aplicadas para paliar posibles efectos negativos sobre interesados
- Documentadas
- Si entraña alto riesgo, también notificación a los afectados para que puedan protegerse

Códigos de conducta

Sirven para especificar el modo en que se va a cumplir con el Reglamento para un determinado sector de actividad. Similar a códigos tipo actuales.

- Obligación de promoción para los EEMM, APD, Comité y Comisión para correcta aplicación del Reglamento
- Asociaciones y organismos representativos de categorías de responsables o encargados podrán promover códigos de conducta para especificar la aplicación del Reglamento.

El Reglamento recoge un contenido indicativo de los códigos:

- Intereses legítimos que persiguen los responsables del tratamiento en contextos específicos
- Recogida de datos personales, pseudonimización
- Información proporcionada al público y a interesados
- Ejercicio de los derechos
- Transferencias internacionales …….

Certificaciones

- Certificaciones, sellos y marcas aplicables a responsables y encargados
- Obligación de promoción para los EEMM, APD, Comité y Comisión para correcta aplicación del Reglamento.
- Objeto: Demostrar el cumplimiento de lo dispuesto en el Reglamento en las operaciones de tratamiento y permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes
- Son voluntarias, se expedirán por periodos máximos de 3 años y son renovables
- El organismo de certificación o la APD podrá retirar la certificación en caso de incumplimiento
- El Comité llevará un registro de todos los mecanismos de certificación, sellos y marcas, que pondrá a disposición del público por cualquier medio apropiado

Certificaciones

¿Quién puede emitir y renovar una certificación?

- APD
- Un organismo de certificación que tenga un nivel adecuado de pericia en materia de protección de datos, una vez informada la APD a fin de que pueda ejercer sus poderes de verificación (retirar una certificación, ordenar al organismo que retire una certificación o que no emita una certificación sin no cumple con requisitos para la certificación)

Los EEMM garantizarán que los organismos de certificación sean acreditados por:

- Autoridad de control competente según los art. 55 y 56 (APD)
- Organismo de acreditación designado de acuerdo con el Reglamento 765/2008 del Parlamento Europeo y del Consejo con arreglo a la norma ISO 17065/2012 y los requisitos adicionales que establezca la APD
- Ambos

¡Muchas gracias por su atención!