El nuevo Reglamento Europeo de Protección de Datos

M. Rosario Heras Carrasco
Responsable de la Unidad de Evaluación y Estudios Tecnológicos
Agencia Española de Protección de Datos

INDICE

- Evaluaciones de impacto
- Consulta previa
- Códigos de conducta
- Certificaciones

Evaluaciones de impacto

LEGISLACION ACTUAL

- 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.

Evaluaciones de impacto

REGLAMENTO EUROPEO PROTECCION DATOS

- RESPONSABILIDAD ACTIVA: Prevé que los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento de los datos personales se lleva a cabo de conformidad con el Reglamento.
- Teniendo en cuenta la naturaleza, el ámbito, contexto y fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos fundamentales.
- Deben estar en condiciones de demostrar el cumplimiento.
- Son medida revisables y se actualizarán cuando sea necesario.
- Considera insuficiente “no incumplir”.
- Incluye obligaciones dirigidas a prevenir incumplimientos.

Evaluaciones de impacto

TIPOS DE MEDIDAS (9)

- Mantener registro de actividades de tratamiento
- Protección de Datos desde el diseño
- Protección de Datos por defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo una evaluación de impacto
- Autorización previa o consultas previas con la APD
- Designación Delegado de Protección de Datos (DPO)
- Notificación de quiebras de seguridad
- Códigos de conducta y esquemas de certificación

Tienen un carácter preventivo, medidas que eviten el incumplimiento. No medidas para cumplir

Evaluaciones de impacto

ENFOQUE DE RIESGO

- Medidas aplicables en función del riesgo para derechos y libertades de los interesados
- El riesgo no es sólo medidas de seguridad

Los riesgos para los derechos y libertades de las personas físicas pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los **casos en los que el tratamiento pueda 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

- En los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales
- Cuando los datos personales tratados 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 o en los caso en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran numero de interesados.

Evaluaciones de impacto

¿Cuándo hay que hacer una evaluación de impacto?

Cuando sea probable que el tratamiento previsto presente un alto riesgo específico para los derechos y libertades de los interesados, entre otros casos, cuando

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas basada en un tratamiento automatizado, como elaboración de perfiles 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

Evaluaciones de impacto

Gran Escala

- ✓ Operaciones que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y
- ✓ Que podrían afectar a un gran número de interesados y
- ✓ Entrañen probablemente un alto riesgo
- ✓ Cuando estas operaciones hagan difícil para los interesados el ejercicio de sus derechos

Observación Sistemática

Control de zonas de acceso público a gran escala, usando dispositivos optoelectrónicos o cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe un alto riesgo para los derechos y libertades y particularmente si impide a los interesados ejercer un derecho, utilizar un servicio o ejecutar un contrato o porque se efectúe a gran escala (considerando 91)

Evaluaciones de impacto

¿Qué es una evaluación de impacto?

- Es algo más que la mera comprobación del cumplimiento normativo.
- Debe realizarse con anterioridad a la implantación de un nuevo producto o servicio o sistema de información.
- Proceso sistemático para evaluar los riesgos existentes para la privacidad de las personas y su nivel de impacto.
- Permite analizar los riesgos que un determinado sistema de información, producto o servicio puede entrañar y gestionar los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.
- Debe ser sistemática y reproducible.
- Orientada a procesos más que a producir un informe final.
- Debe permitir identificar de forma clara a los responsables de las distintas tareas.

Evaluaciones de impacto

Fases para realizar una evaluación de impacto

- Análisis de necesidad
- Descripción del proyecto y de los flujos de información. Categorías de datos, flujos de información y tecnologías utilizadas.
- Identificación de los riesgos para la protección de datos. Realización de un análisis de posibles riesgos valorando la probabilidad de que sucedan y daño que causarían si se materializan.
- Consulta con partes afectadas por el proyecto.
- Gestión de los riesgos identificados. Determinar controles y medidas que deben adoptarse para eliminar, mitigar, transferir o aceptar los riesgos detectados.
- Informe final. Riesgos y recomendaciones.
- Implantación de recomendaciones.
- Revisión y realimentación.

Consulta APD

- Antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo y
- el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables teniendo en cuenta la tecnología disponible y los costes de aplicación

Información a aportar en la consulta:

- ✓ Responsabilidades del responsable (corresponsables o encargados) implicados en el tratamiento
- ✓ Fines y medios del tratamiento previsto
- ✓ Medidas y garantías que se han establecido para proteger derechos y libertades de los interesados
- ✓ Datos de contacto del DPO
- ✓ Evaluación impacto
- ✓ Cualquier otra información que solicite la APD

Consulta APD

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)

El derecho nacional podrá establecer consulta y petición de autorización previa en tratamientos derivados del ejercicio de una misión realizada en interés público (protección social y salud pública)

Códigos de conducta

Para un determinado sector de actividad, sirven para especificar el modo en que se va a cumplir con el Reglamento. 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 …….

Códigos de conducta

TRAMITACION

- Se presenta ante la “autoridad competente” que lo aprobará, registrará y publicará siempre que considere que ofrece garantías suficientes.

- Los promotores debe consultar a las partes interesadas incluidos los interesados cuando sea posible.

- Si un proyecto de código guarda relación con actividades de tratamiento en varios EEMM, la autoridad de control que sea competente en base al mecanismo de coherencia, lo presentará al Comité que será quien dictamine sobre su conformidad.
- Si el código de conducta se considera correcto, el Comité lo presentará a la Comisión quien, mediante actos de ejecución decidirá si el código es válido en toda la UE y le dará publicidad.

Códigos de conducta

OGANISMO DE SUPERVISION

- Lo permite para supervisar el cumplimiento siempre que tenga el nivel adecuado de pericia en relación con el objeto de código tipo y sin perjuicio de las competencias de la APD
- Si el órgano de supervisión existe debe ser acreditado por la APD siguiendo criterios que han de ser aprobados por el Comité.
- Criterios que deben cumplir para acreditarse:
  - Independencia y pericia
  - Establecimiento de procedimientos de evaluación y supervisión de su aplicación
  - Procedimientos para atender reclamaciones de los interesados
  - Demostrar ausencia de conflicto de intereses
- APD podrá retirar acreditación o sancionar al organismo

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

Certificaciones

Criterios de acreditación de organismos de certificación

- Demostrar ante la APD su independencia y competencia en relación con el objeto de la certificación
- Comprometerse a respetar los criterios de certificación aprobados por la APD
- Establecer procedimientos para emitir, revisar y retirar certificaciones
- Establecer procedimientos y estructuras para tratar reclamaciones relativas a infracciones de la certificación
- Han demostrado ante la APE que sus funciones y cometidos no dan lugar a conflicto de intereses

La acreditación de la entidad de certificación se expedirá por un máximo de cinco años y puede ser renovada en las mismas condiciones.

¿Quién aprueba estos criterios?

- La APD
- Comité. Certificación común denominada “Sello Europeo de Protección de Datos”

Certificaciones

Los organismos de certificación serán responsables de la correcta evaluación a efectos de emitir o retirar una certificación sin perjuicio de la responsabilidad del responsable o encargado del tratamiento respecto del cumplimiento del Reglamento.

Los organismos de certificación comunicarán a las autoridades de control las razones por las que expiden o retiran una certificación.

Las autoridades de control o el organismo de acreditación pueden revocar la acreditación de un organismo de certificación si las condiciones de acreditación no se cumplen o han dejado de cumplirse.

¡Muchas gracias por su atención!