11ª Conferencia Internacional sobre la Reutilización de la información del Sector Público

Julián Prieto Hergueta

Agencia Española de Protección de Datos

Madrid, 28 de noviembre de 2019

RESPONSABILIDAD PROACTIVA

El RGPD incorpora dos enfoques fundamentales que inspiran la regulación del derecho fundamental a la protección de datos y que suponen un cambio en el modelo de cumplimiento por parte de los sujetos obligados:

- **EL ENFOQUE DE PROACTIVIDAD O "ACCOUNTABILITY"**
- **EL ENFOQUE DE LA EVALUACIÓN DEL RIESGO**

La responsabilidad proactiva surge del concepto de origen anglosajón, ACCOUNTABILITY, complejo y de difícil traslación al derecho continental, pues engloba aspectos como la asunción y determinación de responsabilidades, la transparencia, la rendición de cuentas, pero que sustancialmente refiere a la aplicación de la normativa de protección de datos y poder demostrarla

RESPONSABILIDAD PROACTIVA

El concepto de responsabilidad proactiva exige que las organizaciones:

- **Apliquen y cumplan los requisitos que establece la regulación de protección de datos**
- **Sean capaces de demostrar ese cumplimiento**

El RGPD lo recoge en las siguientes previsiones:

- **Como principio de actuación en el art. 5.2 RGPD: el responsable del tratamiento será responsable del cumplimiento de los principios y capaz de demostrarlo (responsabilidad proactiva o accountability)**

- **Art. 24.1 RGPD: 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**

PRINCIPIOS


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

PRINCIPIOS

❑ … y el de Responsabilidad Proactiva.

El RGPD 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.La no aplicación de estas medidas es sancionable

Tipos de medidas de cumplimiento

- ❑ Registro de actividades de tratamiento
- ❑ Protección de Datos desde el Diseño y por Defecto
- ❑ Análisis de riesgos, evaluaciones de impacto, consulta a las autoridades de control y Medidas de seguridad
- ❑ Notificación de Quiebras de Seguridad
- ❑ Delegado de Protección de Datos (DPD)
- ❑ **CÓDIGOS DE CONDUCTA** y certificaciones

MEDIDAS DE RESPONSABILIDAD PROACTIVA

MEDIDAS DE RESPONSABILIDAD PROACTIVA

VOLUNTARIAS

- Evaluaciones de Impacto
- Delegado Protección de Datos
- Códigos de conducta
- Certificaciones

CÓDIGOS DE CONDUCTA

NO SON UNA NOVEDAD

- DIRECTIVA 95/46 (art. 27)
- LOPD (art. 32)
- RLOPD
  - ✓ Contenido (arts. 71 – 78)
  - ✓ Procedimiento (arts. 145 – 152)

REGULACIÓN APLICABLE

- RGPD (arts. 40 y 41)
- PLOPD (art. 38 y disposición adicional segunda)
- PROCEDIMIENTOS (RLOPD arts. 145 – 152)
- DIRECTRICES 1/2019 del Comité Europeo de Protección de Datos (CEPD)

CÓDIGOS DE CONDUCTA

Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento (considerando 98).

CÓDIGOS DE CONDUCTA

- **Facilitan la correcta aplicación del RGPD, teniendo en cuenta las características específicas de los distintos sectores y las necesidades específicas de PYMES y micropymes**
- **Método práctico para alcanzar un alto nivel de protección y garantía del derecho de protección de datos**
- **Pueden aportar garantías adecuadas para las transferencias internacionales de datos**
- **Tienen carácter voluntario. Sólo obligan a quienes se comprometan a aplicar sus disposiciones**
- **Útil y efectiva herramienta de accountability**

CÓDIGOS DE CONDUCTA

Su objeto es especificar la aplicación del RGPD, como en lo que respecta a:

- ✓ **El tratamiento leal y transparente**
- ✓ **Los intereses legítimos de los responsables**
- ✓ **La recogida de datos personales**
- ✓ **La seudonimización de datos**
- ✓ **La información a facilitar al público y a los usuarios**
- ✓ **Los derechos de los interesados**
- ✓ **La información a niños y cómo obtener el consentimiento o tutela de los padres o tutores**
- ✓ **La responsabilidad del responsable, PbD y por defecto, y medidas de seguridad**
- ✓ **Las notificaciones de brechas de seguridad**
- ✓ **Las transferencias internacionales.**
- ✓ **Procedimientos extrajudiciales y de mediación para la resolución de conflictos, sin perjuicio actuaciones APD y Tribunales**

Obligatorio: Los mecanismos de control del cumplimiento del Código, sin perjuicio competencias APD

CÓDIGOS DE CONDUCTA

ADMISIBILIDAD DE LOS CÓDIGOS DE CONDUCTA (DIRECTRICES)

- Memoria explicativa que indique su ámbito de aplicación, las específicas características del sector en materia de protección de datos y cómo facilitar la efectiva aplicación del RGPD
- Legitimidad: número de miembros potenciales, experiencia en el sector de actividad
- Ámbito material de aplicación (operaciones de tratamiento)
- Ámbito territorial
- Mecanismos de supervisión
- Organismo de supervisión
- Información sobre las consultas llevadas a cabo
- Cumplimiento normativa nacional

CÓDIGOS DE CONDUCTA

CRITERIOS DE APROBACIÓN (DIRECTRICES)

- Servir para necesidades particulares del tratamiento de datos en sector de actividad correspondiente
- Facilitar la aplicación del RGPD
- Especificar la aplicación del RGPD
- Proporcionar garantías suficientes
- Incluir mecanismos efectivos para el control de su cumplimiento (auditorías, informes periódicos, procedimientos de gestión de reclamaciones, sanciones y remedios de los daños causado, procedimientos para reportar brechas de seguridad...)
- **NO SE TRATA DE REPETIR EL RGPD, SINO QUE DEBEN CONTRIBUIR A LA ADECUADA APLICACIÓN DEL RGPD AL SECTOR DE TRATAMIENTO DE QUE SE TRATE Y CONSTITUIR UN VALOR AÑADIDO. HAN DER TENER CALIDAD Y CONSISTENCIA INTERNA**

CÓDIGOS DE CONDUCTA

PROCEDIMIENTOS DE ELABORACIÓN Y ADOPCIÓN

Elaboración por las asociaciones u organizaciones (promotores) que deben consultar con todas las partes interesadas, incluidos los interesados cuando sea posible y tener en cuenta sus consideraciones. Conforme a la LOPDPGDD también los pueden presentar: empresas, grupos de empresas, entidades de resolución extrajudicial de conflictos y por el sector público: AAPP, Universidades públicas…

• CÓDIGOS DE ÁMBITO EXCLUSIVAMENTE NACIONAL –La autoridad de protección de datos competente evaluará si es conforme al RGPD y si ofrece garantías suficientes y lo aprobará
–Publicidad y Registro del Código por la APD

• CÓDIGOS QUE AFECTAN A TRATAMIENTOS EN VARIOS ESTADOS UE –La APD competente, antes de su aprobación, lo enviará al CEPD para:

a) dictamen sobre su adecuación al RGPD (el art. 64.1 sólo hace referencia a este tipo de decisión en el mecanismo de coherencia) y/o
b) dictamen sobre las garantías ofrecidas para las T.I.D.

- El CEPD enviará el dictamen favorable a la Comisión, que decidirá sobre si el código tiene validez dentro de la UE y, en ese caso, le dará publicidad,
- El CEPD llevará un registro de los códigos y los pondrá a disposición pública

CÓDIGOS DE CONDUCTA

SUPERVISIÓN

- **El control obligatorio de cumplimiento del código podrá ser llevado a cabo por un organismo con el nivel de pericia adecuado en relación con el objeto del código y que haya sido ACREDITADO POR LA APD COMPETENTE**
- **Tomará medidas adecuadas en caso de infracción del código (suspensión o expulsión del infractor del código)**
- **Informará de las sanciones y de los motivos a la APD competente**
- **El incumplimiento de sus obligaciones implica sanción de hasta 10 M. €**
- **No se aplica a los códigos del sector público**

CÓDIGOS DE CONDUCTA

ACREDITACIÓN DE LOS ORGANISMOS DE SUPERVISIÓN

Se podrá acreditar a un organismo de supervisión si:

- **Demuestra independencia y pericia en el objeto del código**
- **Establece procedimientos para evaluar la idoneidad de los responsables y encargados para aplicar el código, supervisar su cumplimiento y examinar periódicamente su aplicación**
- **Establece procedimientos y estructuras para tramitar reclamaciones que sean transparentes para los interesados y el público**
- **Demuestra que no hay conflicto de intereses**

La APD revocará la acreditación si no se cumplen las condiciones de acreditación o si el organismo infringe el RGPD

CÓDIGOS DE CONDUCTA

ACREDITACIÓN DE LOS ORGANISMOS DE SUPERVISIÓN (DIRECTRICES)

- **INDEPENDENCIA**
  - **EXTERNO O INTERNO (independiente de la organización del promotor: staff, presupuesto, función y responsabilidad separada)**
- **AUSENCIA CONFLICTO DE INTERESES**
- **EXPERIENCIA PARA LLEVAR A CABO SUS FUNCIONES**
- **ESTABLECIMIENTO DE PROCEDIMIENTOS Y ESTRUCTURAS para determinar la idoneidad de los adheridos, supervisar el cumplimiento del código y revisar las operaciones del código (auditorías, inspecciones, informes, cuestionarios)**
- **ESTABLECIMIENTO DE PROCEDIMIENTOS Y ESTRUCTURAS para tramitar las reclamaciones de manera imparcial y transparente**
- **COMUNICACIÓN CON LA AUTORIDAD DE CONTROL. Es el contacto con la autoridad de control para cualquier asunto relacionado con el código**
- **MECANISMOS DE REVISIÓN para asegurar que el código sigue siendo relevante y contribuye a la adecuada aplicación del RGPD, y adaptarse a los cambios que se puedan producir**
- **ESTATUTO LEGAL**

CÓDIGOS DE CONDUCTA

EFECTOS

- **Podrá servir de elemento para demostrar el cumplimiento de las obligaciones del responsable**
- **El cumplimiento de los códigos se tendrá en cuenta a efectos de evaluar el impacto en protección de datos de las operaciones de tratamiento (PIAS)**
- **Podrá servir de elemento para demostrar el cumplimiento de las obligaciones sobre medidas de seguridad**
- **Podrá servir de elemento para demostrar que el encargado adherido a un código ofrece garantías suficientes (encargado o subencargado)**
- **Garantías suficientes para realizar T.I.D.**
- **Se tendrá en cuenta a la hora de sancionar**

agencia española protección datos

MUCHAS GRACIAS

www.aepd.es

@AEPD_es