8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA, CERTIFICACIONES Y TRANSFERENCIAS INTERNACIONALES

Julián Prieto Hergueta
Subdirector General del Registro General de Protección de Datos

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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**
- **Aportan garantías adecuadas para las transferencias internacionales de datos**
- **Tienen carácter voluntario. Sólo obligan a quienes se comprometan a aplicar sus disposiciones**
- **Los Estados, APDs, CEPD y la Comisión obligados a impulsar su elaboración**

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA

ÁMBITO DE APLICACIÓN

SUBJETIVO: **Asociaciones y organismos representativos de categorías de RESPONSABLES O ENCARGADOS del tratamiento, incluidas las Administraciones Públicas**

Posibilidad adhesión responsables o encargados no sujetos al RGPD para garantías T.I.D.

OBJETIVO: **correcta aplicación del RGPD en los distintos ámbitos sectoriales**

TERRITORIAL:

- **Códigos nacionales**
- **Códigos que afecten a tratamientos en varios Estados UE**

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA

CONTENIDO

Habrá de especificar la aplicación del RGPD, entre otra la relativa 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.**
- **Los procedimientos de resolución de conflictos, sin perjuicio actuaciones APD y Tribunales**
- **Los mecanismos de control del cumplimiento del Código, sin perjuicio competencias APD**

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

- **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**

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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 tratamientos públicos

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA

ACREDITACIÓN DE LOS ORGANISMOS DE SUPERVISIÓN

Las APD competentes fijarán los criterios de acreditación y los someterán al CEPD para su dictamen a través del mecanismo de coherencia

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

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CÓDIGOS DE CONDUCTA

Inscritos actualmente en el Registro General de Protección de Datos

Código Tipo de Fichero Histórico de Seguros del Automóvil (UNESPA)	2000
Código Tipo de Unió Catalana D'Hospitals (UCH)	2002
Código Tipo de Comercio Electrónico y Publicidad Interactiva (AUTOCONTROL-AECE-IAB SPAIN)	2002
Código Tipo de Odontólogos y Estomatólogos de España	2004
Código Tipo Universidad de Castilla-La Mancha	2004
Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA)	2004
Código Tipo del Sector de la Intermediación Inmobiliaria. Asociación Empresarial de Gestión Inmobililaria (AEGI)	2004
Código Tipo Farmaindustria	2009
Código Tipo del Fichero de Automóviles de Pérdida Total, Robo e Incendios (UNESPA)	2011
Código Tipo para el tratamiento de datos de carácter personal para establecimientos sanitarios privados de la provincia de Sevilla (REAL E ILUSTRE COLEGIO DE FARMACÉUTICOS DE SEVILLA)	2011

CÓDIGOS DE CONDUCTA

Código Tipo de protección de datos personales del fichero ASNEF PROTECCIÓN (ASNEF PROTECCIÓN)	2015
Código Tipo del tratamiento de datos de carácter personal aplicable al tratamiento de datos de la Oficina de Farmacia (Colegio de Farmacéuticos de Barcelona)	2015
Código Tipo para el tratamiento de datos de carácter personal (ASOCIACIÓN NACIONAL DE ENTIDADES DE GESTIÓN DE COBRO-ANGECO)	2015
Código Tipo de protección de datos para Organizaciones Sanitarias	2016

Inscritos en Registros Autonómicos de Protección de Datos e incluidos en el Registro General de Protección de Datos

Código Tipo para las entidades locales adheridas a EUDEL (Asociación de Municipios Vascos-Euskadiko Udalen Elkartea)	2009

ADAPTACIÓN: MODIFICACIÓN

CERTIFICACIONES, SELLOS Y MARCAS

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

- **Objeto:**
  - **Demostrar el cumplimiento del RGPD por responsables y encargados y/o**
  - **Proporcionar garantías adecuadas para las T.I.D.**
  - **De manera que permitan evaluar con mayor rapidez el nivel de protección de datos de productos y servicios**

- **Se tendrán en cuanta las necesidades específicas de las PYMES y micropymes**

- **No limitará la responsabilidad de los responsables o encargados en cuanto al cumplimiento del RGPD, con arreglo a las competencias de las APD**

- **Carácter voluntario y disponible de manera transparente**

- **Los Estados, APDs, CEPD y la Comisión obligados a impulsar su elaboración, especialmente en el ámbito de la UE**

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

- **Expedición de la certificación por:**
  - **Un organismo de certificación acreditado**
  - **La APD competente**
  - **CEPD**

- **Criterios de certificación han de ser aprobados por:**
  - **La APD competente**
  - **CEPD, que dará lugar una certificación común: Sello Europeo de Protección de Datos**

- **Los responsables y encargados facilitarán toda la información y acceso a las actividades de tratamiento al organismo de certificación**

- **Validez por 3 años, renovable en las mismas condiciones**

- **La expedición y renovación de una certificación por un organismo de certificación habrá de comunicarse previamente a la APD, que podrá retirarla u ordenar que no se expida**

- **Se retirará por el organismo de certificación, y en su caso por la APD, si no se cumplen los requisitos de la certificación**

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

ORGANISMOS DE CERTIFICACIÓN

- Tendrán un nivel adecuado de pericia en protección de datos y estar acreditados por

ORGANISMOS DE ACREDITACIÓN

  - La APD competente y/o
  - El organismo nacional de acreditación (ENAC Reglamento 765/2008) con arreglo a la norma EN ISO/IEC 17065/2012 y los requisitos establecidos por la APD competente
  - El CEPD

- Criterios de acreditación aprobados por:
  - La APD competente
  - El CEPD

Cuando se trate de organismos nacionales de acreditación, estos criterios complementarán a los del Reglamento (CE) 765/2008 y las normas técnicas de los métodos y procedimientos de los organismos de certificación

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

ACREDITACIÓN DE LOS ORGANISMOS DE CERTIFICACIÓN

- Se acreditarán organismos de certificación si:
  - Demuestran independencia y pericia en el objeto de la certificación
  - Se comprometen a respetar los criterios de certificación
  - Establecen procedimientos para la expedición, revisión periódica y retirada de certificaciones, sellos y marcas
  - Establecen procedimientos y estructuras para tramitar reclamaciones relativas a infracciones de la certificación por responsables/encargados, que sean transparentes para los interesados y el público
  - Demuestran que no hay conflicto de intereses
- La acreditación es válida por 5 años máximo, renovable en las mismas condiciones. La APD competente o el organismo nacional las revocarán si no se cumplen las condiciones de la acreditación o si el organismo de certificación incumple el RGPD

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

ORGANISMOS DE CERTIFICACIÓN

- **Responsables de la correcta evaluación de la certificación y de su retirada. No exime a los responsables o encargados de responsabilidad por el incumplimiento del RGPD**

- **El CEPD dispondrá de un registro público de los certificados, sellos y marcas, los organismos acreditados y responsables y encargados acreditados (certificados) establecidos en terceros países cuando sirven de garantías para las T.I.D.**

- **El incumplimiento de sus obligaciones es sancionable con de hasta 10 M. €**

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

- **Las APD harán públicos los criterios y requisitos de acreditación y de certificación de forma fácilmente accesible y los comunicarán al CEPD**

- **La Comisión podrá adoptar actos delegados para especificar las condiciones a tener en cuenta en los mecanismos de certificación en materia de protección de datos, previo dictamen del CEPD sobre los requisitos de certificación**

- **La Comisión podrá establecer normas técnicas para los certificados, sellos y marcas y mecanismos para promoverlos y reconocerlos (actos de ejecución)**

MECANISMOS DE CERTIFICACIÓN, SELLOS Y MARCAS

EFECTOS

- Podrá servir de elemento para demostrar el cumplimiento de las obligaciones del responsable
- Elemento que acredite el cumplimiento de la privacidad desde el diseño y por defecto
- Podrá servir de elemento para demostrar el cumplimiento de las obligaciones sobre medidas de seguridad
- Podrá utilizarse como elemento para demostrar que los encargados/subencargados ofrecen garantías suficientes
- Garantías suficientes para realizar T.I. de datos
- Se tendrá en cuenta a la hora de sancionar

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

TRANSFERENCIAS INTERNACIONALES

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

TRANSFERENCIAS INTERNACIONALES DE DATOS

T.I.D. EN EL RGPD

Nivel Adecuado

- Países
- Territorios
- Sectores
- Organismos Internacionales

Garantías adecuadas

- Instrumento jurídico vinculante y exigible entre Autoridades
- BCR
- Cláusulas tipo (Comisión)
- Cláusulas tipo (APD + Comisión)
- Código de Conducta
- Mecanismo de certificación
- Contrato “Ad hoc”
- Acuerdos administrativos entre Autoridades

Excepciones art. 49

- Consentimiento del interesado
- Contrato entre interesado y responsable
- (…)
- Interés legítimo del responsable o encargado

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

TRANSFERENCIAS INTERNACIONALES DE DATOS

TRANSFERENCIAS NO AUTORIZADAS: las transferencias o comunicaciones solicitadas por sentencia judicial o decisión de autoridades administrativas sólo serán reconocidas como ejecutables si se basan en un acuerdo internacional vigente entre el país tercero y la UE o un EM, sin perjuicio de las demás causas que legitiman las transferencias

TRANSFERENCIAS INTERNACIONALES DE DATOS

NIVEL ADECUADO DE PROTECCIÓN

DECISIÓN EXCLUSIVA DE LA COMISIÓN EUROPEA ATENDIENDO AL

- **ESTADO DE DERECHO**

  Legislación pertinente, general y sectorial: Seguridad pública, defensa y seguridad nacionales y penal, acceso autoridades a los datos (su aplicación)

  Normas sobre protección de datos profesionales y medidas de seguridad

  Jurisprudencia

  Derechos efectivos y exigibles (recursos administrativos y judiciales efectivos)

- **APD INDEPENDIENTES**

  Garanticen cumplimiento normativa

  Poder de ejecución (sancionador)

  Asistan, asesoren a los interesados y cooperen con APD de la UE y de los EM

- **COMPROMISOS INTERNACIONALES ASUMIDOS**

  Participación sistemas multilaterales o regionales sobre protección de datos

8ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

TRANSFERENCIAS INTERNACIONALES DE DATOS

NIVEL ADECUADO DE PROTECCIÓN

- La decisión establecerá un mecanismo de revisión periódica, al menos cada 4 años
- La Comisión debe consultar al CEPD
- La Comisión supervisa y evalúa su aplicación informando al CEPD y al P.E.

LAS DECISIONES DE ADECUACIÓN ADOPTADAS POR LA COMISIÓN EUROPEA SEGÚN LA DIRECTIVA 95/46 MANTENDRÁN SU VIGENCIA HASTA SU MODIFICACIÓN, SUSTITUCIÓN O DEROGACIÓN

- Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda
- Canadá (ley canadiense Personal Information and Electronic Documents Act)
- USA (SAFE HARBOUR) INVALIDADA TJUE. PRÓXIMO PRIVACY SHIELD

TRANSFERENCIAS INTERNACIONALES DE DATOS

GARANTÍAS ADECUADAS

a) Instrumento jurídicamente vinculante y exigible entre autoridades y organismos públicos

b) BCR

c) Cláusulas estándar adoptadas por la Comisión Europea

d) Cláusulas estándar adoptadas por una APD y aprobadas por la Comisión (el art. 64.1.d las incluye en el sistema de coherencia)

e) Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o encargado en el tercer país, por vía contractual o por instrumento jurídicamente vinculante para aplicar las garantías, incluidas las de los derechos de los interesados

f) Mecanismos de certificación (igual que los códigos de conducta)

g) Cláusulas “ad hoc” entre el exportador e importador. Requiere autorización de las APD que las someterá al mecanismo de coherencia

h) Acuerdos administrativos entre autoridades y organismos públicos que incluyan derechos efectivos y exigibles para los interesados (MoU). Requiere autorización APD y mecanismo de coherencia (el art. 64.1 no lo contempla)

Las decisiones de la Comisión sobre cláusulas estándar adoptadas continuarán en vigor hasta su modificación, sustitución o derogación

TRANSFERENCIAS INTERNACIONALES DE DATOS

BCR

- RECONOCIDAS POR PRIMERA VEZ EN LA NORMATIVA DE PROTECCIÓN DE DATOS EUROPEA
- SE CONFIGURAN COMO UNA DE LAS GARANTÍAS APROPIADAS PARA PODER REALIZAR TRANSFERENCIAS INTERNACIONALES DE DATOS SIN NECESIDAD DE AUTORIZACIÓN ESPECÍFICA
- NO DISTINGUE ENTRE BCR DE RESPONSABLES Y DE ENCARGADOS
- APROBACIÓN POR LA AUTORIDAD DE CONTROL COMPETENTE POR EL MECANISMO DE COHERENCIA
- REQUISITOS
  - Jurídicamente vinculantes: todos los miembros del grupo incluidos empleados
  - Derechos a los afectados
  - Cumplan el contenido mínimo

TRANSFERENCIAS INTERNACIONALES DE DATOS

CONTENIDO MÍNIMO BCR

- Estructura del Grupo y datos de contacto de todos sus miembros
- Transferencias, datos, afectados, tratamientos, fines, destino
- Carácter jurídicamente vinculante
- Principios protección de datos (limitación finalidad, conservación, calidad, PbD y por defecto, transferencias ulteriores…)
- Derechos afectados y medios para ejercerlos en los EM
- Aceptación responsabilidad por actuación de miembros fuera UE
- Forma de informar de las BCR a los interesados
- Funciones DPO
- Procedimientos de reclamación
- Mecanismos para garantizar la verificación del cumplimiento (auditorías y acciones correctivas)
- Procedimiento para su modificación y comunicación
- Mecanismos cooperación e información a las APD
- Formación del personal en protección de datos

TRANSFERENCIAS INTERNACIONALES DE DATOS

EXCEPCIONES

- Consentimiento del interesado, previa información sobre los posibles riesgos
- Ejecución contrato entre interesado y responsable (medidas precontractuales)
- Celebración o ejecución contrato en interés del afectado entre el responsable y un tercero
- Motivos importantes de interés público (establecido por Ley nacional o europea)
- Ejercicio o defensa de reclamaciones
- Interés vital del afectado o de terceros cuando el interesado está incapacitado
- Desde un registro público con arreglo al derecho de la Unión o de los EM

Interés legítimo del responsable sobre el que no prevalezcan los derechos y libertades del interesado, no repetitivas, limitadas, evaluación circunstancias y ofrecimiento garantías apropiadas (se informará a las APD y al interesado)

TRANSFERENCIAS INTERNACIONALES DE DATOS

SIN NECESIDAD DE AUTORIZACIÓN ESPECÍFICA

- A países, territorios, sectores u organismos internacionales declarados de nivel adecuado de protección
- BCR
- Cláusulas tipo adoptadas por la Comisión
- Cláusulas tipo adoptadas por una APD y aprobadas por Comisión
- Instrumento jurídicamente vinculante entre autoridades públicas
- Mecanismos de certificación
- Códigos de conducta
- Excepciones

NECESIDAD DE AUTORIZACIÓN POR LAS APD

- Contratos “ad hoc”
- Acuerdos administrativos entre autoridades públicas

NOTIFICACIÓN AEPD Y AL INTERESADO

- Intereses legítimos prevalentes del responsable

LAS AUTORIZACIONES OTORGADAS Y TRANSFERENCIAS A PAÍSES DE NIVEL ADECUADO REALIZADAS VIGENTES HASTA SU MODIFICACIÓN, SUSTITUCIÓN O DEROGACIÓN

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es