

# **DESARROLLO DE COMPETENCIAS AVANZADAS PARA LA APLICACIÓN DE LA PROTECCIÓN DE DATOS EN LA JUNTA DE ANDALUCÍA**

## **UNIDAD 2**

---

**Otras medidas de responsabilidad activa:  
Delegado de Protección de Datos. Códigos de  
conducta. Certificaciones. Transferencias  
internacionales de datos**

## CONTENIDOS

1.	LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS.....	3
1.1	ANTECEDENTES .....	3
1.2	OBLIGATORIEDAD, PERFIL Y APTITUDES .....	3
1.3	POSICIÓN EN LA ORGANIZACIÓN ADMINISTRATIVA .....	6
1.4	FUNCIONES .....	9
2.	LOS CÓDIGOS DE CONDUCTA EN EL RGPD Y LA LOPDGDD.....	12
2.1	OBJETO Y NATURALEZA .....	17
2.2	SUJETOS LEGITIMADOS.....	18
2.3	CONTENIDO DE LOS CÓDIGOS DE CONDUCTA .....	19
2.4	LAS DIRECTRICES 1/2009 DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS.....	22
2.5	LOS ORGANISMOS DE SUPERVISIÓN .....	24
2.6	APROBACIÓN DE LOS CÓDIGOS DE CONDUCTA .....	27
2.7	BENEFICIOS E INCENTIVOS DE LOS CÓDIGOS DE CONDUCTA .....	29
3.	ESQUEMA DE CERTIFICACIÓN .....	31
3.1	LÍNEAS GENERALES DE LA CERTIFICACIÓN .....	31
3.2	ESPECIAL CONSIDERACIÓN A LA CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS.....	33
4.	TRANSFERENCIAS INTERNACIONALES DE DATOS .....	35
4.1	MARCO GENERAL DE LAS TRANSFERENCIAS .....	35
4.2	TRANSFERENCIAS BASADAS EN UNA DECISIÓN DE ADECUACIÓN .....	38
4.3	TRANSFERENCIAS MEDIANTE GARANTÍAS ADECUADAS .....	38
4.4	NORMAS CORPORATIVAS VINCULANTES .....	39
4.5	EXCEPCIONES PARA SITUACIONES ESPECÍFICAS.....	41



Este curso ha sido cedido por la Agencia Española de Protección de Datos por medio de una licencia Creative Commons Reconocimiento-No comercial-Compartir igual, en los términos que se describen en <http://creativecommons.org/licenses/by-nc-sa/3.0/es> o texto oficial que, para esta modalidad de licencia, sustituya al indicado.

## 1. LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS

### 1.1. ANTECEDENTES

Desde la Unión Europea se ha llevado a cabo una revisión del marco normativo del derecho a la protección de datos fruto de varios factores, entre otros la rápida evolución tecnológica que plantea nuevos retos a la protección de nuestra privacidad, que se ha recogido en el ya conocido Reglamento General de Protección de Datos, aplicable desde el pasado 25 de mayo, y que, junto con la reciente Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, constituye el modelo aplicable en nuestro país.

El RGPD y la Ley Orgánica son de aplicación a las entidades privadas, así como a las autoridades y organismos públicos que realizan tratamientos de datos personales, con la excepción de aquellos que tengan que ver con la seguridad nacional, la política exterior y de seguridad común, y aquellos que son llevados a cabo por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de las sanciones, a las que se aplica la Directiva 680/2016 y la legislación por la que se incorpore a nuestro ordenamiento jurídico.

El Reglamento General de Protección de Datos introduce la figura del delegado de protección de datos como una de las medidas, junto con, entre otras, la necesidad de adoptar un enfoque basado en el riesgo, la elaboración del registro de actividades de tratamiento, la adopción de medidas de protección de datos desde el diseño y por defecto, el establecimiento de las adecuadas medidas de seguridad, la notificación de brechas de seguridad, en su caso la evaluación de impacto sobre la privacidad, para poner en práctica el principio de responsabilidad proactiva.

Este principio de responsabilidad proactiva y el enfoque basado en el riesgo son dos de los mayores retos que se recogen en el Reglamento europeo y que requieren un mayor esfuerzo por parte de los responsables y encargados del tratamiento y en los que el delegado de protección de datos debe jugar un papel fundamental a la hora de asesorar al responsable y supervisar el cumplimiento de la normativa de protección de datos dentro de la organización.

Es por tanto un elemento central para cumplir con el objetivo de facilitar el cumplimiento del marco normativo de protección de datos mediante la aplicación de instrumentos de rendición de cuentas y actuar como intermediarios entre las partes interesadas correspondientes.

### 1.2. OBLIGATORIEDAD, PERFIL Y APTITUDES

El RGPD regula de forma detallada el Delegado de Protección de Datos en los artículos 37 a 39, sin perjuicio de que aparece mencionado en otras partes del articulado, así como en los considerandos de la norma, estableciendo una serie de supuestos de designación obligatoria por parte de los responsables y encargados:

- El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

- Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

El Grupo de autoridades de protección de datos del Artículo 29 de la Directiva 95/46/CE, y que en el marco del RGPD ha dado paso al Comité Europeo de Protección de Datos, a través del documento [“Directrices sobre los delegados de la protección de datos”](#), ha precisado lo siguiente sobre el supuesto de obligatoriedad en los Administraciones públicas:

*El RGPD no define qué se considera como “**autoridad u organismo público**” por lo que tal noción debe determinarse de conformidad con la legislación de cada país, que, si bien se entienden incluidas las autoridades nacionales, regionales y locales, también pueden ser incluidos otros organismos regidos por el derecho público. Respecto a las organizaciones privadas que participen a través de las diferentes modalidades de contratación de la gestión de los servicios público, si bien no sería obligatorio la designación del delegado de protección de datos, se recomienda como buena práctica su nombramiento, cubriendo su actividad no sólo los tratamientos relacionados con esa gestión pública sino también los que no lo estén.*

El apartado 4 del artículo 37 del RGPD abre la posibilidad de que los países de la Unión, a través de su normativa específica puedan establecer otros supuestos en que haya que nombrar a un delegado de protección de datos.

En este sentido, y aprovechando esta posibilidad, la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos de Personales y garantía de los derechos digitales, especifica con mayor detalle el alcance de esta previsión del Reglamento.

- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los

responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de estos.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
- Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Las federaciones deportivas cuando traten datos de menores de edad.



Además, el apartado 2 de este artículo 34 de la Ley Orgánica 3/2018 recoge, **sin perjuicio de estos supuestos** de obligatoriedad, **la posibilidad de que exista una designación voluntaria** de un delegado de protección de datos.

Por otra parte, el RGPD determina que el Delegado de Protección de Datos en su artículo 37.5 y considerando 97 será una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos. La Ley Orgánica 3/2018 señala que el cumplimiento de estos requisitos para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

En el citado anteriormente documento “[Directrices sobre los delegados de la protección de datos](#)”, figuran al respecto las siguientes precisiones:

- **Conocimiento:**  
Aunque el Reglamento General de Protección de Datos no lo define, el nivel de conocimiento debe ser acorde con el tipo, cantidad y complejidad de datos que trate una organización.
- **Cualificación profesional:**  
Tampoco está precisado en el Reglamento General de Protección de Datos. No obstante, el Delegado de Protección de Datos debe tener conocimiento de las leyes tanto nacionales como europeas, así como del mencionado Reglamento. En el ámbito privado, debe conocer el sector empresarial y en el ámbito público, un conocimiento sólido de las normas y procedimientos administrativos.
- **Capacidad:**  
Para desempeñar sus tareas debe tenerse en cuenta tanto sus cualidades personales y sus conocimientos como el puesto que ocupe en la organización. Entre las de carácter personal, se incluirían la integridad y un nivel elevado de ética profesional.

### 1.3. POSICIÓN EN LA ORGANIZACIÓN ADMINISTRATIVA

Como hemos visto en el apartado anterior, el RGPD determina la obligatoriedad de designar un Delegado de Protección de Datos en el ámbito de las Administraciones públicas. En el documento “[El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones públicas](#)”, la AEPD considera como uno de los impactos sobre las citadas Administraciones sobre la aplicación de la norma la necesidad de designar un Delegado de Protección de Datos:

*“El RGPD prevé que todas las “autoridades u organismos públicos” nombrarán un DPD. También establece cuáles habrán de ser los criterios para su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.*

*En consecuencia, como medida previa deben identificarse las unidades en que se integra el DPD dentro de cada órgano u organismo, su posición en la estructura administrativa y los mecanismos para asegurar que los DPD designados reúnen los requisitos de cualificación y competencia establecidos por el RGPD.*

*La designación del DPD debe comunicarse a las autoridades de protección de datos. Asimismo, deben establecerse mecanismos para que los interesados puedan contactar con el DPD”.*

Con carácter general, cabe señalar, en primer lugar, que de acuerdo con el RGPD es posible designar un único delegado para, por ejemplo, un ministerio, consejería o ayuntamiento.

Al mismo tiempo, no parece aconsejable que ese único delegado actúe respecto de grandes unidades u órganos con entidad y tareas claramente diferenciadas, por mucho que orgánicamente puedan depender



de un departamento ministerial, consejería o ayuntamiento (podrían ser ejemplos los casos de la Secretaría de Estado de Seguridad Social, responsable de la dirección y tutela de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, o el de la Dirección General de Tráfico).

Por otra parte, y dadas las funciones del Delegado de Protección de Datos, su adscripción dentro de la estructura de la organización debe hacerse a órganos o unidades con competencias y funciones de carácter horizontal. Asimismo, el nivel del puesto de trabajo debe ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones.

El RGPD prevé que el delegado podrá desarrollar su actividad a tiempo completo o parcial y también que podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

En órganos, organismos o entes de gran tamaño en que exista un único delegado lo habitual será que desempeñe sus funciones a tiempo completo. Es, incluso, posible que el delegado formalmente nombrado esté respaldado por una unidad específicamente dedicada a la protección de datos.

En entidades de menor tamaño será posible que el delegado compagine sus funciones con otras. Si éste es el caso, debe tenerse en cuenta la necesidad de evitar conflictos de intereses entre las diversas ocupaciones.

Además, debe tenerse en cuenta que el delegado actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de TIC, o responsables de seguridad de la información).

El RGPD también ofrece la posibilidad de que se contraten externamente las funciones de delegado. Esta opción puede ser utilizada en determinados casos, como podría ser el de pequeños municipios que se benefician de un servicio que ofrezca una diputación provincial o una comunidad autónoma o, incluso, que donde ese servicio no exista puedan optar por los servicios de entidades privadas especializadas.

Por otra parte, es necesario analizar cuál es la posición del Delegado de Protección de Datos en el marco de la organización donde presta sus servicios.

En este sentido, el RGPD se refiere en su artículo 38 a cuál es el encuadre del delegado en el marco de la entidad en la que haya sido designado:

- La participación de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales;
- Recibir el apoyo del responsable o encargado, que deberán facilitarle los recursos necesarios para el desempeño de sus funciones;
- No recibir ninguna instrucción en lo que respecta al desempeño de dichas funciones y no ser destituido ni sancionado por el responsable o el encargado por causas relacionadas con ese desempeño de funciones;
- Rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado. Esta característica debe interpretarse en el sentido de que el delegado debe poder relacionarse con niveles jerárquicos que tengan la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones que realice;

- Invitar al delegado a participar con regularidad en las reuniones de los cuadros directivos altos y medios;
- Presencia en la toma de decisiones con implicaciones para la protección de datos, de forma que toda la información relevante se le transmita de manera oportuna para que pueda prestar un asesoramiento adecuado;
- Su opinión debe gozar siempre de la consideración oportuna, documentando las razones para no seguir su consejo;
- Se le debe consultar tan pronto se produzca una violación de datos u otro incidente;

Además, según el documento del Grupo del Artículo 29 “[Directrices sobre los Delegados de Protección de Datos](#)”, debe tenerse en consideración los elementos referentes:

- **Recursos:** El artículo 38.2 del Reglamento determina que la organización debe apoyar al delegado proporcionándole los recursos necesarios para realizar sus funciones, así como el acceso a los datos personales y operaciones de tratamiento, así como para mantener su conocimiento experto. Por parte de la alta dirección, debe existir un apoyo activo a las funciones que realice el delegado, como el tiempo suficiente para el ejercicio de las mismas; dotación de recursos económicos, infraestructura y personal; acceso a otros servicios (recursos humanos, departamento jurídico, tecnologías de la información) que puedan apoyar al delegado; y equipo de personas a cargo del delegado en función de la estructura de la organización.
- **Independencia:** El artículo 38.3 del Reglamento establece unas garantías básicas para que los delegados actúen con independencia dentro de la organización en la que prestan sus servicios, incluyendo que “no reciban ninguna instrucción relativa al ejercicio de sus tareas”. Además, es importante señalar que los obligados al cumplimiento del RGPD son el responsable o el encargado del tratamiento, de forma que, si adoptan decisiones contrarias a la norma y al asesoramiento prestado por el delegado, debe darse a éste la posibilidad de expresar con claridad su opinión disconforme respecto a dichas decisiones.
- **Destitución:** El anteriormente citado artículo 38.3 también se refiere a que los Delegados de Protección de Datos “no deben ser destituidos ni penalizados por el responsable o el encargado por llevar a cabo sus funciones”, lo que supone un refuerzo de su autonomía e independencia. Sí podría ser despedido o sancionado de conformidad con la legislación contractual, laboral o penal aplicable de cada país, por causas distintas al desempeño de sus funciones (por ejemplo, por robo o acoso sexual). Téngase en cuenta en el ámbito de las Administraciones públicas el régimen de infracciones y sanciones aplicables a su personal.
- **Conflicto de interés:** Si bien el Delegado de Protección de Datos puede realizar otras funciones en la organización, éstas no pueden suponer un conflicto de intereses. Por ello, y atendiendo a la estructura, actividades y tamaño de cada organización, se recomienda que responsables o encargados del tratamiento: determinen los puestos que serían incompatibles con las funciones del Delegado; elaboren normas internas para evitar estos conflictos; declarar que el Delegado no tiene conflicto de intereses en relación con sus funciones; inclusión de salvaguardas en normas internas y garantizar que el anuncio de la vacante para Delegado o el contrato de servicios sea lo suficientemente preciso y detallado para evitar los citados conflictos.

A este respecto, la Ley Orgánica 3/2018 recoge, en su artículo 36, lo siguiente:



- El delegado de protección de datos actuará como interlocutor del responsable o encargado de tratamiento ante la AEPD y las autoridades autonómicas de protección de datos.
- Si se trata de una persona física, no podrá ser removido ni sancionado por el responsable o el encargado en desempeñar sus funciones salvo que incurriera en dolo o negligencia.
- En el ejercicio de sus funciones tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado la existencia de cualquier deber de confidencialidad o secreto.
- Cuando el delegado aprecie la existencia de una vulneración relevante en materia de protección de datos lo comunicará inmediatamente a los órganos de administración y dirección del responsable o encargado.

## 1.4. FUNCIONES

Las funciones del Delegado de Protección de Datos, que serán de información, asesoramiento y supervisión, se encuentran especificadas en el artículo 39 del RGPD, y que según el documento de la AEPD [“El Delegado de Protección de Datos en las Administraciones Públicas”](#), las mismas se pueden concretar en las siguientes áreas:

- **RESPECTO AL CUMPLIMIENTO:**
  - Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
  - Identificación de las bases jurídicas de los tratamientos.
  - Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
  - Existencia de normativa sectorial que pueda determinar condiciones de tratamientos específicos distintas de las establecidas por la normativa general de protección de datos.
  - Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable- encargado.
  - Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
  - Diseño e implantación de políticas de protección de datos.
  - Auditoría de protección de datos.
  - Establecimiento y gestión de los registros de actividades de tratamiento.
- **RESPECTO A LA RELACIÓN CON LOS INTERESADOS:**
  - Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
  - Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
  - Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- **RESPECTO A LA SEGURIDAD:**
  - Análisis de riesgo de los tratamientos realizados.

- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- **RESPECTO A LA PREVENCIÓN:**
  - Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
  - Realización de evaluaciones de impacto sobre la protección de datos.
  - Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- **RESPECTO A LA COOPERACIÓN:**
  - Relaciones con las autoridades de supervisión.
- **RESPECTO A LA FORMACIÓN:**
  - Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

Además de los preceptos del Reglamento, a los que hemos hecho referencia sobre la regulación del Delegado de Protección de Datos, la norma se refiere al delegado en otros apartados de la misma:

- **En el derecho de información (artículos 13 y 14):** Contempla la posibilidad de que cuando se recaben los datos de carácter personal de los interesados, se les facilite, en el caso de que haya sido designado, los datos de contacto del Delegado de Protección de Datos.
- **En el Registro de Actividades (artículo 30):** Que deben implementar tanto el responsable como el encargado, también tendrían que figurar los citados datos de contacto.
- **Notificaciones de brechas de seguridad (artículo 33):** Debe incluirse con la finalidad de poder obtener más información sobre la brecha ocurrida, los datos de contacto del delegado.
- **Evaluaciones de Impacto de Protección de Datos (artículo 35):** Obligación de que el responsable recabe el asesoramiento del Delegado de Protección de Datos a la hora de realizar estas Evaluaciones. Cuando una vez realizada la Evaluación de Impacto, el tratamiento de datos pueda suponer un alto riesgo si no se mitigan los daños, y por tanto, el responsable debe consultar al respecto a la Autoridad de Control, cuando realice dicha consulta se incluirán los datos de contacto del Delegado de Protección de Datos.
- **Normas corporativas vinculantes (artículo 47):** En su contenido mínimo se reflejará las funciones del Delegado de Protección de Datos.
- **Relación con las Autoridades de Control de Protección de Datos (artículo 57.3):** Las relaciones entre el Delegado de Protección de Datos y su respectiva Autoridad de Control serán gratuitas, sin coste económico que tenga que sufragar la entidad que haya designado al delegado.

Con respecto a la capacidad para desempeñar las funciones indicadas en el artículo 39 del RGPD, es preciso señalar la capacidad de servir de enlace tanto entre los miembros de los órganos de dirección de su organización (39.1.a RGPD), como enlace con el personal de su organización (39.1 b RGPD), como con la autoridad de control (39.1 d y e) como con los interesados (38.4 RGPD).

Por otra parte, la Ley Orgánica de Protección de Datos introduce, en su artículo 37, la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

Según el citado precepto:

- El afectado podrá con carácter previo a la presentación de una reclamación dirigirse al delegado de protección de datos de la entidad contra la que se reclame.
- En este caso, el delegado comunicará al afectado la decisión que hubiera adoptado en un plazo máximo de dos meses a contar desde la recepción de la reclamación.
- Si el afectado presenta una reclamación ante la AEPD o, en su caso, autoridades autonómicas de protección de datos, sin haber hecho uso de la citada posibilidad, aquéllas podrán remitir la reclamación al delegado a fin de que éste responda en el plazo de un mes. Si transcurrido este plazo el delegado no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento.

Como resumen de las previsiones que afectan a las Administraciones Públicas en relación con la designación del Delegado de Protección de Datos se pueden señalar:

- **Designación.** Las autoridades y organismo públicos tienen la obligación de designar un DPD con la cualificación recogida en el artículo 35 de la Ley y en el Reglamento General de Protección de Datos, garantizando sus funciones dentro de la organización. Es obligatorio facilitar los datos de contacto del delegado a los ciudadanos, así como comunicarlo a la Agencia Española de Protección de Datos.
- **Intervención.** Los ciudadanos podrán, antes de presentar una reclamación ante la Agencia, dirigirse al Delegado de Protección de Datos para que la atienda. El DPD comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses. Se trata de promover la celeridad en la resolución de las reclamaciones que plantea el ciudadano, que puede ver resuelto su caso en un plazo más breve que si hubiera que iniciar un expediente administrativo. Asimismo, cuando el ciudadano presente una reclamación ante la Agencia ésta podrá remitir la reclamación al DPD para que éste responda en el plazo de un mes. Con ello, se persigue que el ciudadano obtenga una resolución rápida del conflicto planteado, aunque, si pasado el plazo no responde, la autoridad de protección de datos continuará con el procedimiento.
- **Responsabilidad.** El Delegado de Protección de Datos no tiene responsabilidad a título personal de las posibles infracciones cometidas por la organización en la que desempeñe sus funciones.

## 2. LOS CÓDIGOS DE CONDUCTA EN EL RGPD Y LA LOPDGDD

Los códigos de conducta constituyen una manifestación de la capacidad de autorregulación de las organizaciones por la que se vinculan y obligan al cumplimiento de pautas de actuación, conductas y normas en el ejercicio de su actividad.

En materia de protección de datos personales, con la denominación de códigos tipo, ya se reconocían en la primera ley de protección de datos, la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, la LORTAD, que, en su artículo 31<sup>1</sup>, se refería a los códigos tipo como mecanismos de autorregulación para facilitar a determinados sectores de actividad la adaptación y el cumplimiento de la normativa de protección de datos de carácter y les atribuía el carácter de códigos deontológicos o de buena práctica profesional.

El reconocimiento de los códigos de conducta continuó en las siguientes normas que en materia de protección de datos se fueron adoptando, tanto en el ámbito europeo, en el artículo 27 de la Directiva 95/46/CE<sup>2</sup>, como en el nacional, a través del artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), que vino a reproducir casi en su integridad el artículo 31 de la LORTAD; y de su Reglamento de desarrollo, aprobado por el Real Decreto, 1720/2007, de 21 de diciembre, en sus artículos 71 a 78, sobre el contenido de los códigos y las obligaciones de sus promotores, y 145 a 152, sobre el procedimiento de inscripción en la Agencia Española de Protección de Datos.

Marco jurídico a cuyo amparo se elaboraron e inscribieron en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos un total de 18 códigos tipo<sup>3</sup>.

<sup>1</sup> Artículo 31. Códigos tipo.

1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo.

Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

<sup>2</sup> Artículo 27

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representativas de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.

Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo

29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

<sup>3</sup> - Código Tipo Fichero Histórico de Seguros del Automóvil (UNESPA)

- Código Tipo de la Unión Catalana de Hospitales (UCH)

- Comercio Electrónico y Publicidad Interactiva (AUTOCONTROL-AECE-IAB SPAIN)

- Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España (Consejo General de Colegios Oficiales de Odontólogos y Estomatólogos de España)

- Código Tipo de Protección de Datos Personales en la Universidad de Castilla-La Mancha (UCLM)

- Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA)

Ni el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, o RGPD), ni la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD) proporcionan una definición de código de conducta. Más allá del carácter de buena práctica profesional que les atribuía la LORTAD y la LOPD de 1999, el Grupo de Trabajo del Artículo 29<sup>4</sup>, en su documento sobre “Evaluación de la autorregulación industrial” (WP7), adoptado el 14 de enero de 1998, proporciona, a los efectos de determinar el nivel de protección en un país tercero para la realización de transferencias internacionales de datos, una amplia definición de “autorregulación” aplicable a los códigos de conducta al indicar que “deberá entenderse por código de autorregulación cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente

por miembros del sector industrial o profesión en cuestión”.

No obstante, la ausencia de definición de código de conducta, el RGPD en el artículo 40 regula su contenido, alcance y aprobación, y en el 41 su control a través del correspondiente organismo de supervisión. La LOPDPGDD, a su vez, ha continuado con la tradición de regular en el ámbito nacional los códigos de conducta en su artículo 38, en la medida que el RGPD permite la intervención del derecho interno para su desarrollo y complemento, sin perjuicio de su aplicación directa en todos los Estados miembros de la UE desde el 25 de mayo de 2018.

## RGPD

### Artículo 40. Códigos de Conducta

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

- 
- Código Tipo del Sector de la Intermediación Inmobiliaria (Asociación Empresarial de Gestión Inmobiliaria -AEGI-)
  - Código Tipo de Farmaindustria de Protección de Datos Personales en el Ámbito de la Investigación Clínica y de la Farmacovigilancia (FARMAINDUSTRIA)
  - Código Tipo del Fichero de Automóviles de Pérdida Total, Robo e Incendios (UNESPA)
  - Código Tipo de Tratamiento de Datos de Carácter Personal para Establecimientos Sanitarios Privados de la Provincia de Sevilla (Colegio de Farmacéuticos de Sevilla)
  - Código Tipo de Protección de Datos Personales del Fichero ASNEF PROTECCIÓN (ASNEF)
  - Código Tipo del Tratamiento de Datos de Carácter Personal Aplicable al Tratamiento de Datos de la Oficina de Farmacia (Colegio de Farmacéuticos de la provincia de Barcelona)
  - Código Tipo para el Tratamiento de Datos de Carácter Personal de la Asociación Nacional de Entidades de Gestión de Cobro (ANGECO)
  - Código Tipo de Protección de Datos para Organizaciones Sanitarias Privadas
  - Código Tipo del Fichero de Prevención del Fraude en Seguros de Ramos Diversos (UNESPA)
  - Código Tipo de Protección de Datos de Carácter Personal de la Universidad Nacional de Educación a Distancia (UNED)
  - Código de Conducta para el Tratamiento de Datos de Carácter Personal por Organizaciones de Investigación de Mercados, Social y de la Opinión y del Análisis de Datos (ANEIMO y AEDEMO)
  - Código Tipo de la Asociación Española de Micropréstamos (AEMIP)

<sup>4</sup> Grupo que reúne a las autoridades de protección de datos de los Estados miembros de la UE, de las instituciones europeas y a la Comisión Europea, creado en el artículo 29 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los datos (Directiva 95/46)



2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

- a) el tratamiento leal y transparente;
- b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
- c) la recogida de datos personales;
- d) la seudonimización de datos personales;
- e) la información proporcionada al público y a los interesados;
- f) el ejercicio de los derechos de los interesados;
- g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
- h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;
- i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
- j) la transferencia de datos personales a terceros países u organizaciones internacionales, o
- k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.
7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.
8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.
9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.
10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.
11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

#### **Artículo 41. Supervisión de códigos de conducta aprobados**

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.
2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:
  - a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;
  - b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;
  - c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y
  - d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los criterios de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.
4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.
5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.
6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.”

## **LOPDGDD**

### **Artículo 38. Códigos de conducta.**

1. Los códigos de conducta regulados por la sección 5.<sup>a</sup> del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas, así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.”

## 2.1. OBJETO Y NATURALEZA

El RGPD ha supuesto un cambio de paradigma en el modo de cumplir con la normativa de protección de datos, consecuencia directa de la aplicación del principio de responsabilidad proactiva (accountability) que incorpora, y conforme al cual los responsables del tratamiento no sólo son responsables de su cumplimiento, sino que han de estar en condiciones de poder demostrarlo (artículo 5 RGPD), lo que pone el foco en la diligencia de los sujetos obligados, convirtiéndola en pieza clave del sistema de cumplimiento.

Para facilitar el ejercicio de la responsabilidad proactiva y la actuación diligente de los sujetos obligados, el RGPD prevé diversos instrumentos como los códigos de conducta y los mecanismos de certificación, sellos y marcas, cuyo impulso y promoción se encarga a los Estados miembros, el Comité Europeo, la Comisión Europea y las autoridades de protección de datos.

El RGPD configura a los códigos de conducta como una herramienta de accountability que permite demostrar su cumplimiento mediante una regulación dirigida a especificar y contribuir a su correcta aplicación, teniendo en cuenta las características específicas de los distintos sectores de actividad que realizan tratamiento de datos.

El considerando 98 del RGPD señala que se debe incitar a la elaboración de 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.

Los Códigos de conducta constituyen una regulación complementaria al RGPD y a la LOPDPGDD, que conforman la normativa indisponible en materia de protección de datos que ha de ser respetada, cuya finalidad, en atención a las peculiaridades y necesidades específicas de la actividad de los distintos sujetos obligados, es facilitarles su cumplimiento en aquellos aspectos que las disposiciones legales al ser de carácter transversal puedan necesitar ser completadas. En protección de datos los códigos de conducta no sustituyen a la normativa aplicable, sino que la complementan, desarrollan sus principios y refuerzan las garantías que ofrece a los interesados, lo que los convierte en una herramienta apropiada de accountability de carácter voluntario.

Ya se ha indicado que la decisión de elaboración de los códigos de conducta responde a la capacidad de autorregulación de las organizaciones que deciden adoptarlos de manera voluntaria. Son instrumentos fruto de la voluntad de sus promotores, sin que ni el RGPD ni la LOPDPGDD impongan ninguna obligación de elaboración a responsables o encargados. La única obligación que imponen es la de su fomento y promoción a los poderes públicos, en particular entre las microempresas y las pequeñas y medianas empresas.

Del mismo modo, también es voluntaria la adhesión de responsables y encargados a los códigos de conducta. Determinadas organizaciones a la hora de elaborar un código de conducta lo convierten en obligatorio para todos sus integrantes, lo que, en su caso, determinará la salida de la organización de aquellas entidades que no quisieran vincularse a las disposiciones del código de conducta.

Las estipulaciones de los códigos de conducta, una vez aprobados por la autoridad de protección de datos competente, se convierten en vinculantes para todos aquellos que voluntariamente se adhieran al código, y cuyo incumplimiento implica la aplicación de su propio régimen sancionador.

Los códigos de conducta pueden ser de alcance nacional o doméstico, o transnacional, cuando guarden relación con actividades de tratamiento en varios Estados miembros, lo que implica la intervención del CEPD en su aprobación que ha de dictaminar si son conformes con el RGPD.

## 2.2. SUJETOS LEGITIMADOS

El RGPD da un paso más allá de lo dispuesto en el artículo 27 de la Directiva 45/96, que se refería a las asociaciones profesionales y demás organizaciones representantes de otras categorías de responsables de tratamientos como promotores de códigos de conducta, dejando olvidados a los encargados, algo que en el ámbito español no fue obstáculo para que se inscribieran en la Agencia Española de Protección de Datos códigos tipo que regulaban el tratamiento de datos por encargados<sup>5</sup>.

El artículo 40 del RGPD señala que “Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta...”. Incluye ya a los encargados del tratamiento, a través de sus organizaciones, entre los sujetos legitimados para poder presentar códigos de conducta. El artículo 28.5 del RGPD, la elección por un responsable del tratamiento

<sup>5</sup> Código Tipo para el Tratamiento de Datos de Carácter Personal de la Asociación Nacional de Entidades de Gestión de Cobro (ANGECO)



de un encargado adherido a un código de conducta le sirve de elemento para demostrar la diligencia que debe mostrar para que sea un encargado que ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme al RGPD y garantice la protección de los derechos del interesado.

La LOPDPGDD, en su artículo 38, ha ampliado el ámbito de los sujetos legitimados a las empresas o grupo de empresas, así como a las instituciones del sector público relacionadas en su artículo 77.1, entre ellas los órganos constitucionales, las Administraciones públicas, o las universidades públicas<sup>6</sup>, dos de éstas últimas ya contaban con un código tipo, y en el ámbito de la Agencia Vasca de Protección de Datos se llegó a contar con un código tipo de los Ayuntamientos vascos.

Además de estos sujetos, que siguen la línea de la LOPD de 1999, lo que constituye una novedad es la previsión de que puedan ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del RGPD.

El citado artículo hace referencia a los organismos de supervisión de los códigos de conducta, de los que hablaremos más adelante, que para ser acreditados han de demostrar entre otros elementos que disponen de procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público.

Con ello, la LOPDPGDD ha querido mantener el ámbito de los códigos de conducta que ya se recogía en la LOPD de 1999 y ampliarlo a los organismos de resolución extrajudicial de conflictos para conseguir que los responsables o encargados que se adhieran al código de conducta se obliguen a someter a dichos organismos las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado.

## 2.3. CONTENIDO DE LOS CÓDIGOS DE CONDUCTA

Una de las principales novedades que, con respecto a la normativa anterior, introduce el RGPD es la relativa a su contenido.

<sup>6</sup> Los responsables o encargados recogidos en el artículo 77.1 de la LOPDPGDD son los siguientes:

- Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos
- Los órganos jurisdiccionales
- La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local
- Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas
- Las autoridades administrativas independientes
- El Banco de España
- Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público
- Las fundaciones del sector público
- Las Universidades Públicas
- Los consorcios

El Reglamento de desarrollo de la LOPD de 1999 permitía al promotor decidir si el código tipo se aplicaba a todos o sólo a algunos de los tratamientos de datos que realizasen los adheridos, salvo si era un código de empresa en cuyo caso debía regular todos los tratamientos, pero en ambos casos se exigía una regulación completa que debía incluir todos los aspectos de los tratamientos incluidos en su ámbito de aplicación material. Los códigos tipo debían incluir el contenido al que se hacía referencia en el artículo 73 del Reglamento de la LOPD, que implicaba todo el ciclo de vida de los datos personales, un procedimiento de supervisión y una relación de adheridos, conforme a lo que disponían los artículos 75 y 76. Además, cabía la opción de incluir compromisos adicionales.

Frente a esta regulación, el RGPD, en su artículo 40.2, incluye una relación enunciativa no exhaustiva de materias sobre las que podrán versar los códigos de conducta, al disponer que se podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del RGPD, en particular en lo que respecta a:

- a) el tratamiento leal y transparente;
- b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
- c) la recogida de datos personales;
- d) la seudonimización de datos personales;
- e) la información proporcionada al público y a los interesados;
- f) el ejercicio de los derechos de los interesados;
- g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
- h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;
- i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
- j) la transferencia de datos personales a terceros países u organizaciones internacionales, o
- k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

Esta relación no constituye un contenido mínimo, a diferencia de lo que establecía el Reglamento de la LOPD de 1999, o de lo que el propio RGPD en su artículo 47 establece para las normas corporativas vinculantes (BCR), que son un instrumento de características similares a los códigos de conducta. Esto implica un cambio de modelo para los promotores de los códigos que podrán limitarlos a regular exclusivamente aquellos aspectos que respondan a las necesidades que el tratamiento de datos presenta en un determinado sector de actividad, o, con arreglo al artículo 38 de la LOPDPGDD, para un determinado responsable.

Este diferente enfoque permite la elaboración de códigos de conducta que atiendan a varios o a uno solo de los aspectos relacionados, como, por ejemplo, el tratamiento de los datos de menores de edad, la seudonimización de los datos personales, las transferencias internacionales de datos, o los procedimientos extrajudiciales de resolución de conflictos. Como recoge el considerando 98 del RGPD “los 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”.

Por tanto, los códigos de conducta podrán especificar la aplicación del RGPD en lo que respecta a cualquiera de estos aspectos, así como a cualquier otro regulado en el propio Reglamento, al ser meramente enunciativa la expresión “como en lo que respecta a”, lo que deja abierta la puerta a la posibilidad de elaborar de códigos de conducta que traten cuestiones distintas de las recogidas en esta relación, como pudieran ser las cesiones de datos, la protección de personas con discapacidad o cualquier otra que tenga por finalidad la aplicación apropiada y efectiva del RGPD.

Lo que sí han de incluir obligatoriamente son los mecanismos de supervisión de su cumplimiento. El artículo 40.4 del RGPD dispone que los códigos de conducta contendrán los mecanismos que permitan al organismo de supervisión efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo.

En consecuencia, sea cual sea el contenido material de los códigos de conducta no pueden obviar incluir los mecanismos para el control de su cumplimiento, ya se trate de códigos aplicables a responsables o encargados del sector privado, como a los promovidos por autoridades y organismos públicos<sup>7</sup>.

La regulación del RGPD introduce en esta relación no exhaustiva dos aspectos que suponen una novedad con respecto a la normativa anterior.

Por una parte, la posibilidad de que los códigos de conducta sirvan como instrumento que incorporen las garantías adecuadas en el marco de las transferencias internacionales de datos, que incluyan derechos de los interesados exigibles y acciones legales efectivas.

En estos supuestos, en los que los destinatarios de los flujos internacionales de datos, responsables o encargados del tratamiento no están sujetos al RGPD por encontrarse fuera de su ámbito de aplicación, éstos han de asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, como la adhesión al código de conducta, para aplicar las garantías adecuadas.

Los códigos de conducta que, independientemente de su ámbito doméstico o transnacional, incluyan garantías para realizar transferencias internacionales de datos exigen para su aprobación por la autoridad de control competente el previo dictamen del CEPD, con arreglo al procedimiento de coherencia, según dispone el artículo 40.7 del RGPD, exigencia que guarda coherencia con lo que se dispone en el artículo 46.2.h) y

3.a) para la aprobación de cláusulas modelo por las autoridades de control, o la autorización de transferencias internacionales basadas en cláusulas contractuales “ad hoc”, respectivamente.

La segunda novedad a destacar es la posibilidad de que los códigos de conducta incorporen procedimientos extrajudiciales y otros procedimientos de resolución de controversias entre los responsables del tratamiento y los interesados relativas al tratamiento de sus datos, con la finalidad de obtener una rápida y justa solución a la controversia.

Hay que diferenciar estos procedimientos de los que deben disponer los organismos de supervisión del cumplimiento de los códigos de conducta para tratar las reclamaciones relativas a infracciones del propio código, o a la manera en que se aplica o se haya aplicado tanto por un responsable como por un encargado del tratamiento (artículo 41.2.c RGPD).

<sup>7</sup> Los recogidos en el artículo 77.1 de la LOPDPGDD

No obstante, es posible que la tramitación de ambos tipos de reclamaciones se asuma por el organismo de supervisión que cada código de conducta ha de incluir, de manera que no sólo atiendan las reclamaciones que sobre su cumplimiento se puedan formular, sino también las controversias entre los afectados y los adheridos al código de conducta que puedan surgir en materia de protección de datos.

Cabe concluir este apartado insistiendo en que la autorregulación no puede entenderse como la promulgación voluntaria de códigos de conducta que se limiten a transcribir lo que disponen las normas de obligado cumplimiento. Para que los códigos puedan cumplir con su finalidad es preciso que no se limiten a ser una mera reproducción de las disposiciones legales, sino que incorporen normas de valor añadido, tanto en lo que se refiere a la articulación de soluciones apropiadas para el sector de actividad de que se trate, o al incremento de garantías legalmente exigibles, como en lo que afecta a los mecanismos internos que garanticen su aplicación efectiva por parte de las entidades voluntariamente adheridas<sup>8</sup>.

Valor añadido que también destacó el Grupo de Trabajo del Artículo 29 en relación con los proyectos de códigos comunitarios en su documento sobre la “Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo” (WP 13)<sup>9</sup>, en el que se dispone que “Los proyectos prematuros y los proyectos que no se ajusten a los requisitos previstos en los apartados 2.1 a 2.3 (que hacen referencia a la legitimación para presentarlo, a su cuidadosa elaboración -previa consulta a los interesados a los que los datos se refiere o a sus representantes- y la lengua en la que se han de redactar) no serán admitidos por el Grupo de Trabajo”.

Un aspecto relacionado directamente con el contenido de los códigos tipo es el relativo a su redacción. El Reglamento de desarrollo de la LOPD de 1999 especificaba que los códigos tipo deberían redactarse en términos claros y accesibles, pues deben ser comprensibles no sólo para las personas encargadas de su aplicación y cumplimiento (responsables y encargados), sino también para el público en general, que incluye a los titulares de los datos objeto de tratamiento, por lo que resulta esencial que los códigos de conducta estén dotados de la claridad y precisión suficiente que permita su observancia y comprensión.

## 2.4. LAS DIRECTRICES 1/2009 DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

Transcurrida la fase de consulta pública, el Comité Europeo de Protección de Datos (CEPD) adoptó, el 4 de junio de 2019, las Directrices 1/2019, sobre los códigos de conducta del RGPD y sus organismos de supervisión (en adelante las Directrices)<sup>10</sup>.

El objetivo de las Directrices es proporcionar asistencia y criterios para la aplicación de las disposiciones de RGPD sobre los códigos de conducta y sus organismos de supervisión. Recoge los requisitos mínimos que han de cumplir los códigos de conducta para que las autoridades de control procedan a su revisión, análisis y aprobación, así como los elementos que, relativos al contenido, han de tener en cuenta en la evaluación de si facilitan y contribuyen a la efectiva aplicación del RGPD; y los requisitos para la supervisión efectiva del cumplimiento del código.

<sup>8</sup> BLANCO ANTÓN, M<sup>a</sup> José: Comentarios al Reglamento de la Ley Orgánica de Protección de Datos de Carácter Personal. Editorial Lex Nova 2008

<sup>9</sup> [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp13\\_es.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp13_es.pdf)

<sup>10</sup> [https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under\\_en](https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en)

Las Directrices indican los requisitos de admisibilidad de los proyectos de códigos de conducta, cuya inobservancia da lugar a su rechazo indicando al promotor las carencias del proyecto presentado.

Los proyectos de códigos de conducta deben contener y demostrar:

- Una memoria clara y concisa de la finalidad que persigue, su ámbito de aplicación y la explicación de cómo facilita la aplicación efectiva del RGPD. Memoria que incluirá la documentación necesaria cuando sea relevante.
- La representatividad del sector de actividad a la que se refiere el código a través de, entre otros elementos, el número o porcentaje de responsables o encargados que agrupa, o la experiencia del promotor en el sector de actividad de que se trate.
- El ámbito objetivo del código, los tratamientos y/o los aspectos del tratamiento que regula, para los que ha de proporcionar soluciones prácticas y efectivas; y el ámbito territorial, en concreto si se trata de un código de ámbito nacional o transnacional, en cuyo caso la tramitación requiere la intervención del CEPD.
- La autoridad de control a la que se dirige el promotor del código para su aprobación, que resulta relevante para el caso de códigos transnacionales.
- Los mecanismos para su control que haya previsto el código.
- El organismo para llevar a cabo la supervisión del código.
- La información que se haya obtenido del proceso de consulta con los actores relevantes del código, o la justificación del por qué no se ha podido realizar la consulta. En el considerando 99 del RGPD se recoge que los promotores de los códigos de conducta “deben consultar a las partes interesadas, incluidos los afectados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas”.
- El cumplimiento de la legislación nacional que resultase aplicable.

Aparte de estos requisitos generales, también se recoge que los proyectos de códigos han de ser presentados, además de en el idioma de la autoridad de control competente, en inglés si se trata de códigos transnacionales, y los criterios para designar la autoridad de control competente.

Así mismo, las Directrices recogen los criterios para la aprobación de los códigos, que hacen referencia a su contenido material. Los promotores de los códigos deberán demostrar que contribuyen a una correcta aplicación del RGPD, en concreto que:

- Dan respuesta a las particulares necesidades del tratamiento de datos en el sector de actividad correspondiente,
- facilitan y especifican la aplicación del RGPD, y
- proporcionan suficientes garantías y mecanismos efectivos para supervisar su cumplimiento.

Un apartado importante de las Directrices es el referido se refieren a los organismos de supervisión de los códigos de conducta y a los requisitos para su acreditación por la autoridad de protección de datos competente que veremos más adelante.

Las directrices también incluyen orientaciones relativas a la presentación de los códigos de conducta ante la autoridad de control, con una relación, o checklist, de los puntos necesarios que debe contener el proyecto<sup>11</sup>, su admisibilidad, tramitación, en particular en el caso de los códigos transnacionales para los

<sup>11</sup> Ver anexo I a estos comentarios



que incluye un diagrama sobre los pasos a dar, aprobación, así como otros aspectos relativos a su seguimiento, publicación y revocación, además de los beneficios que proporcionan.

En definitiva, las Directrices se configuran como un elemento que deben tener presente no sólo las autoridades de control, sino también y muy especialmente los promotores que decidan acometer la tarea de elaborar un código de conducta.

## 2.5. LOS ORGANISMOS DE SUPERVISIÓN

La supervisión del cumplimiento de los códigos de conducta constituye un elemento clave de la autorregulación para evitar que sean percibidos como una mera declaración de intenciones sin fuerza de obligar y cuyo incumplimiento carece de consecuencia alguna ni para el sujeto infractor ni tampoco para los interesados.

Los códigos de conducta han de incluir los mecanismos necesarios para efectuar su control y un organismo para llevarlo a cabo. Forma parte de la naturaleza de la autorregulación el disponer de los instrumentos necesarios para controlar su aplicación y cumplimiento.

El artículo 40.4 del RGPD dispone que los códigos de conducta contendrán mecanismos que permitan al organismo de supervisión, previsto en el artículo 41.1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin que ello excluya las funciones y los poderes de control de las autoridades de control que se podrán desplegar en caso de incumplimiento del RGPD.

El organismo de supervisión lo regula el RGPD en su artículo 41, en unos términos que han dado lugar a diferentes interpretaciones, al disponer que “...podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.”

Por una parte, el artículo 40.4 exige un control del cumplimiento del código por el organismo de supervisión previsto en el artículo 41.1 y, por otra parte, éste precepto utiliza la expresión “podrá”, lo que propició que se planteara la posibilidad de adoptar códigos de conducta sin la necesidad de disponer de un organismo de supervisión acreditado que no prosperó, a pesar de la opinión en este sentido de más de una autoridad de control, pues la Directrices del CEPD claramente indican que la ausencia de un organismo de supervisión acreditado impide la aprobación del código de conducta.

No se puso en duda la existencia de un organismo de supervisión, sino la obligación de acreditarlo que no se aplica respecto de los organismos de supervisión de los códigos de conducta que presenten las autoridades y organismos públicos, los elaborados por las Administraciones públicas, organismos y demás entidades relacionadas en el artículo 77.1 de la LOPDGPDD. Estos códigos de conducta no están exentos de la obligación de incluir mecanismos para el control de su cumplimiento ni, por tanto, de organismos de supervisión, pero sí de ser acreditados por la autoridad de control y del resto de obligaciones del artículo 41 del RGPD.

La acreditación de los organismos de supervisión está reservada en exclusiva a la autoridad de control competente para su aprobación, sin que quepa delegar esta obligación en otras entidades, y el apartado

2 del artículo 41 del RGPD establece los requisitos que deberán reunir los organismos de supervisión para ser acreditados:

- a) Demostrar, a satisfacción de la autoridad de control, su independencia y pericia en relación con el objeto del código;
- b) haber establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;
- c) haber establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y
- d) haber demostrado, a satisfacción de la autoridad de control, que sus funciones y cometidos no dan lugar a conflicto de intereses.

Estos requisitos han sido objeto de exhaustiva atención en las Directrices del CEPD que han identificado los elementos significativos que se han de demostrar y facilitan orientaciones para acreditar su cumplimiento. Estos elementos hacen referencia a:

- La independencia de los organismos de supervisión.
- La ausencia de conflicto de intereses.
- La experiencia y la posesión de conocimientos especializados de las personas que lo integran.
- La existencia de procedimientos y estructura para evaluar la idoneidad de los responsable y encargados que parte del código, supervisar su cumplimiento y realizar revisiones periódicas.
- El establecimiento de procedimientos que garanticen la gestión transparente de las reclamaciones por incumplimiento del código que deberán incluir un régimen sancionador aplicable a los responsables y encargados infractores, sin perjuicio de las competencias de las autoridades de control.
- El establecimiento de los canales de comunicación apropiados con la autoridad de control.
- Los mecanismos para comprobar que el código sigue contribuyendo a la correcta aplicación del RGPD y, en su caso, recomendar su revisión.
- La condición jurídica que permite a las autoridades de control sancionarlos si incumplen las obligaciones que les asigna el RGPD.

En relación con este último elemento, el artículo 41.4 del RGPD estipula que el órgano de control, con las debidas garantías, deberá tomar las medidas oportunas en caso de infracción a lo establecido en el código por uno de los adheridos e informará de ellas y de los motivos para su adopción a la autoridad de control competente. Medidas que comprenden la suspensión o exclusión del código.

Si el organismo de supervisión no cumple con estas obligaciones podrá ser sancionado por la autoridad de control con multa de hasta 10 millones de euros como máximo, o, en el supuesto de que se tratase de una empresa, de una cuantía equivalente al 2% como máximo del volumen del negocio total anual global del ejercicio financiero anterior, debiéndose optar por la de mayor cuantía, según establece el artículo 83.4.c) del RGPD, que en su versión española se recoge como el incumplimiento de “c) Las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.” Evidentemente, se trata de un error de traducción pues, conforme a las definiciones del artículo 4 del RGPD, la autoridad de control es “la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el

artículo 51”, y no se está refiriendo a que la autoridad de control, que es quien detenta la potestad sancionadora, se pueda sancionar a sí misma, sino al organismo de supervisión de los códigos de conducta.

En la versión inglesa del RGPD, el artículo 83.4.c) del RGPD dice lo siguiente “c) The obligations of the monitoring body pursuant to Article 41 (4)”, y las Directrices de CEPD lo dejan claro al recoger que entre los requisitos que han de reunir los organismos de supervisión está el de demostrar que disponen del estatus adecuado para ser susceptibles de sanción conforme al artículo 83.4.c) del RGPD.

Por su parte, la LOPDPGDD en su artículo 70 recoge que están sujetos al régimen sancionador las entidades acreditadas de supervisión de los códigos de conducta, y entre las infracciones sancionables del artículo 73 se incluyen las siguientes:

”ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del (RGPD).”

Error que, no obstante, la corrección de errores que se publicó el 23 de mayo de 2018 en el DOUE, no fue subsanado.

Las autoridades de control, conforme al artículo 41.3 del RGPD, han de someter al CEPD con arreglo al mecanismo de coherencia el proyecto que fije los criterios de acreditación de un organismo de supervisión.

En cumplimiento de dicho precepto, la Agencia Española de Protección de Datos sometió a dictamen del CEPD los criterios de acreditación de los códigos de conducta que finalmente se adoptaron en el mes de febrero de 2020<sup>12</sup>.

En estos criterios se precisan los diferentes elementos puestos de manifiesto por el CEPD en sus Directrices, y se facilitan orientaciones para su acreditación.

La LOPDPGDD ha reforzado el papel de los organismos de supervisión de los códigos de conducta, no sólo admitiéndolos como sujetos legitimados para su elaboración, al disponer en el artículo 38.2 que “Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado...”; y en el 65.4, que “Antes de resolver sobre la admisión a trámite de la (una) reclamación, la Agencia Española de Protección de Datos podrá remitir la misma (...) al organismo de supervisión establecido para la aplicación de los códigos de conducta...”.

Así mismo, dispone que la autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del RGPD.

<sup>12</sup> <https://www.aepd.es/sites/default/files/2020-02/acreditacion-organismos-supervision-cc.pdf>

Como conclusión de este apartado cabe indicar que, si bien la obligación de acreditar a los organismos que han de supervisar el cumplimiento de los códigos de conducta y los deberes que les impone el RGPD pueden llegar a desincentivar su elaboración, tanto las Directrices del CEPD como los Criterios de acreditación fijados por la Agencia Española de Protección de Datos proporcionan la necesaria flexibilidad a los promotores de los códigos de conducta para su elección, interno o externo a la organización o asociación que promueva el código permitiendo la propuesta del que se considere más idóneo.

Finalmente, hay que indicar que la acreditación del organismo de supervisión se revocará por la autoridad de control competente si no se cumplen o hubieran dejado de cumplirse las condiciones de la acreditación, o cuando se infrinja el RGPD.

## 2.6. APROBACIÓN DE LOS CÓDIGOS DE CONDUCTA

El RGPD distingue, en cuanto al procedimiento de aprobación de los códigos de conducta, entre códigos de ámbito exclusivamente doméstico y aquellos que guardan relación con actividades de tratamiento en varios Estados miembros o que incluyen las garantías para realizar transferencias internacionales de datos. Ambos tipos de códigos han de ser aprobados por la autoridad de control competente, si bien para los códigos transnacionales o que sirvan de garantías para las transferencias internacionales de datos se exige que la autoridad de control lo presente al CEPD para su tramitación por el procedimiento de coherencia. El CEPD dictaminará si el código es conforme con el RGPD o, en el caso de las transferencias internacionales, si ofrece las garantías adecuadas (artículo 40.7 RGPD).

En los códigos que regulan actividades de tratamiento en varios Estados miembros, el CEPD presentará su dictamen, si fuera favorable, a la Comisión Europea que, conforme al procedimiento de previsto en el artículo 8 del Reglamento (UE) 182/2011<sup>13</sup> para la adopción de actos de ejecución, podrá decidir que tengan validez general dentro de la UE.

En todo caso, corresponde a la autoridad de control competente, aquella que tiene asignadas las funciones y poderes conforme al RGPD en el territorio de su Estado miembro (artículo 55 RGPD), previo dictamen en su caso del CEPD determinar si el proyecto de código sometido a su aprobación responde al RGPD y si considera suficientes las garantías que ofrece para su aprobación (artículo 40.5 RGPD).

Las Directrices del CEPD, como se ha indicado, incluyen orientaciones relativas al procedimiento de presentación, admisión y aprobación de los códigos de conducta, en particular señalan los requisitos que han de cumplir los proyectos de códigos de conducta para ser presentados, que de no reunirse determinarían la inadmisión del código por la autoridad de control que deberá motivarla<sup>14</sup>.

Por ello, constituye una buena práctica que, antes de su presentación formal, los promotores de los códigos de conducta se dirijan a la autoridad de control competente al objeto darle a conocer su iniciativa y así poderles proporcionar recomendaciones dirigidas a dotar de consistencia al proyecto de código y evitar una presentación prematura.

<sup>13</sup> Reglamento (UE) 182/2011 del Parlamento y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011R0182&from=ES>)

<sup>14</sup> Ver anexo I a estos comentarios

El procedimiento establecido en el RGPD para la aprobación de códigos de conducta hay que completarlo con el de la tramitación interna por parte de las autoridades de control.

La LOPDPGDD en el artículo 38.3 y 4, dispone que los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente. Cuando el proyecto de código de conducta sea transnacional o incorpore las garantías para realizar transferencias internacionales de datos lo someterán al mecanismo de coherencia mencionado que prevé el RGPD para que dictamine el CEPD, quedando suspendido el procedimiento hasta que se emita el dictamen.

Cuando la autoridad de control competente sea autonómica, las comunicaciones con el CEPD se llevarán a cabo por conducto de la Agencia Española de Protección de Datos, conforme dispone el artículo 60 de la propia LOPDPGDD. En estos casos la Agencia Española de Protección de Datos estará asistida por un representante de la Autoridad autonómica en su intervención ante el CEPD.

Un principio básico del RGPD y de la autorregulación es el de transparencia que contribuye a hacer más efectiva su aplicación. En consecuencia, una vez aprobados los códigos de conducta, sus modificaciones o ampliaciones las autoridades de control y el CEPD los archivarán, registrarán y los pondrán a disposición pública. Así mismo, la Comisión Europea dará publicidad adecuada a los códigos sobre los que decida que tienen validez general en la Unión Europea.

La LOPDPGDD, en su artículo 38.5, dispone que “La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos

(...) El registro será accesible a través de medios electrónicos.”

La LOPDPGDD, con la finalidad de facilitar la adaptación de los códigos tipo inscritos en el Registro de la Agencia Española de Protección de Datos, en su Disposición transitoria segunda dispone que:

“Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.”

A la fecha de la redacción de este comentario sobre los códigos de conducta, se encuentran en diferente estado de estudio y tramitación varios proyectos sometidos a la Agencia Española de Protección de Datos para su aprobación, así como las adaptaciones al RGPD de la mayoría de los códigos tipo, cuyos promotores han presentado el correspondiente proyecto en el plazo establecido en la Disposición transitoria segunda de la LOPDPGDD.

Con fecha 09/10/2020 la directora de la AEPD dictó resolución en virtud de la cual se ha aprobado el “CÓDIGO DE CONDUCTA DE TRATAMIENTO DE DATOS EN LA ACTIVIDAD PUBLICITARIA”, cuyo promotor es la ASOCIACIÓN PARA LA AUTORREGULACIÓN DE LA COMUNICACIÓN COMERCIAL “AUTOCONTROL”.

(<https://www.aepd.es/es/documento/codigo-conducta-autocontrol.pdf>).



Asimismo, en la mencionada Resolución se ha acreditado como organismo de supervisión para el código de conducta al Jurado de Publicidad.

El ámbito objetivo o material del mencionado código de conductas lo constituyen los tratamientos o las operaciones de tratamientos de datos con fines publicitarios, en concreto el envío de comunicaciones comerciales; las promociones realizadas con objeto de recoger datos personales para utilizarlos con fines publicitarios; el uso de cookies y tecnologías equivalentes para la gestión de espacios publicitarios o la realización de publicidad comportamental; la elaboración de perfiles con fines publicitarios; y, fundamentalmente, el establecimiento de un procedimiento para la resolución extrajudicial de controversias entre las entidades adheridas y los interesados en materia de protección de datos.

Por otro lado, el plenario del CEPD, reunido el 19 de mayo de 2021, aprobó los dictámenes sobre los códigos de conducta transnacionales de las entidades CISPE (FR) y EU-CLOUD (BE): [https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act\\_es](https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_es).

## 2.7. BENEFICIOS E INCENTIVOS DE LOS CÓDIGOS DE CONDUCTA

El RGPD ha querido dotar de una mayor relevancia a los códigos de conducta, como instrumentos que encajan en el principio de responsabilidad proactiva. No sólo ordena su promoción a distintos poderes y autoridades públicas, sino que a lo largo de su articulado se hace referencia a los efectos que los códigos de conducta producen para los responsables y encargados, que conforman una serie de incentivos que ratifican la apuesta del RGPD por los códigos de conducta.

Las ventajas que proporcionan los códigos de conducta son un factor importante de cara a su desarrollo, que sobre la base de la normativa anterior no se puede decir que hayan tenido una gran aceptación, como se puede apreciar del escaso número de códigos tipo inscritos en el Registro de la Agencia Española de Protección de Datos. Aun cuando se impulsó su desarrollo y se destacó la importancia de la autorregulación para aumentar el grado de conocimiento e implantación del derecho fundamental a la protección de datos<sup>15</sup>, ha de reconocerse que no han tenido el alcance que presumía el Reglamento de la LOPD, según el cual están “llamados a jugar un papel cada vez más relevante como elemento dinamizador del derecho fundamental a la protección de datos”.

Estos incentivos, además de los de índole competitiva y reputacional que pueden representar para las empresas en estos tiempos de continuo desarrollo tecnológico, se recogen en el RGPD. Con carácter general, sirven de elemento para demostrar su cumplimiento por responsables y encargados del tratamiento (artículo 24.3 RGPD), y más en concreto:

- Pueden servir para demostrar el cumplimiento de las obligaciones sobre la seguridad de los tratamientos (artículo 32.3 RGPD).
- El cumplimiento de los códigos de conducta correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por los responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos (artículo 35.8 RGPD).

<sup>15</sup> Memoria de la Agencia Española de Protección de Datos. 2004

- Son un elemento para demostrar que los encargados del tratamiento adheridos a un código de conducta ofrecen las garantías suficientes, de manera que los responsables puedan dar por cumplida su obligación de diligencia en la contratación de los encargados del tratamiento (artículo 28.5 RGPD).
- Pueden proporcionar garantías suficientes para realizar transferencias internacionales de datos (artículo 46.2.e RGPD).
- La adhesión a un código de conducta es un elemento que se tiene en consideración en los supuestos de sanción de multa administrativa (artículo 83.1.j RGPD).

No obstante, y como ya se ha tenido oportunidad de señalar, el disfrute de estos beneficios dependerá del contenido del código, de los aspectos que regule, de manera que, si un determinado código no incluye, por ejemplo, la regulación de las medidas de seguridad no va a poder servir de elemento para demostrar el cumplimiento de los requisitos establecidos a estos efectos por el artículo 32.1 del RGPD.

Por su parte, las Directrices del CEPD señalan que los códigos de conducta representan una oportunidad para establecer reglas que contribuyan a la correcta aplicación del RGPD que tenga en cuenta las características particulares de cada sector, en particular de las medianas, pequeñas y microempresas, de manera transparente, práctica y con reducción de costes; y destaca que pueden:

- ayudar a los responsables y encargados a cumplir el RGPD, ajustándose a las necesidades del sector de actividad de que se trate,
- proporcionar un grado de co-regulación que permita disminuir el nivel de asistencia que responsables y encargados en ocasiones demandan a las autoridades de control,
- proporcionar un grado de autonomía y control a los responsables y encargados para adoptar las mejores prácticas para su sector de actividad, y
- proporcionar confianza y seguridad jurídica mediante la adopción de soluciones prácticas a los problemas identificados por un determinado sector.

No obstante, y como ya se ha tenido oportunidad de señalar, el disfrute de estos beneficios dependerá del contenido del código, de los aspectos que regule, de manera que, si un determinado código no incluye, por ejemplo, la regulación de las medidas de seguridad no va a poder servir de elemento para demostrar el cumplimiento de los requisitos establecidos a estos efectos por el artículo 32.1 del RGPD.

Por su parte, las Directrices del CEPD señalan que los códigos de conducta representan una oportunidad para establecer reglas que contribuyan a la correcta aplicación del RGPD que tenga en cuenta las características particulares de cada sector, en particular de las medianas, pequeñas y microempresas, de manera transparente, práctica y con reducción de costes; y destaca que pueden:

- ayudar a los responsables y encargados a cumplir el RGPD, ajustándose a las necesidades del sector de actividad de que se trate,
- proporcionar un grado de co-regulación que permita disminuir el nivel de asistencia que responsables y encargados en ocasiones demandan a las autoridades de control,
- proporcionar un grado de autonomía y control a los responsables y encargados para adoptar las mejores prácticas para su sector de actividad, y
- proporcionar confianza y seguridad jurídica mediante la adopción de soluciones prácticas a los problemas identificados por un determinado sector.

### 3. ESQUEMA DE CERTIFICACIÓN

#### 3.1. LÍNEAS GENERALES DE LA CERTIFICACIÓN

Como ya hemos visto, el RGPD pone a disposición de los responsables y encargados de tratamientos de datos personales distintas medidas de responsabilidad activa a fin de demostrar el cumplimiento de lo dispuesto en el Reglamento: entre estas medidas está la certificación.

En el considerando 100 del Reglamento se señala expresamente que para aumentar la transparencia y el cumplimiento del mismo debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes. Por ello insta a los Estados miembros, autoridades de control, Comité y Comisión a promover, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento del Reglamento en las operaciones de tratamiento y hace una mención especial a tener en cuenta sobre las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

A este respecto, procede diferenciar lo siguiente:

- **Certificación:** proceso metodológico de evaluación mediante el cual una tercera parte garantiza la conformidad de una persona, un producto, servicio o sistema de información con unos criterios preestablecidos.
- **Esquema de Certificación:** aquel que establece las reglas, los procedimientos y las gestiones que deben realizar aquellas personas, organizaciones públicas o privadas que desean certificarse.

En el caso del RGPD el mecanismo de certificación afecta tanto a responsables como a encargados del tratamiento, es decir, ambos pueden utilizar este mecanismo para garantizar el cumplimiento del mismo. Es importante aclarar que el sólo hecho de que un responsable o encargado disponga de una certificación no limita su responsabilidad en cuanto al cumplimiento por lo que, en su caso, ante una irregularidad la autoridad de control puede ejercer sus funciones y poderes entre los que se encuentra el sancionador.

En este sentido, el RGPD establece entre las funciones de la AEPD algunas relacionadas con las certificaciones:

- Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos y aprobar los criterios de certificación.
- Llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas.

Esta certificación es voluntaria, es decir, ninguna entidad que trate datos personales está obligada a certificarse, por lo que la certificación es un mecanismo opcional que el RGPD pone a disposición de responsables y encargados con el objeto de facilitar el cumplimiento, pero en ningún momento lo establece como una obligación.

Además, la certificación debe estar disponible a través de un proceso transparente y será expedida por los organismos de certificación o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de control o por el Comité teniendo en cuenta que cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común denominada Sello Europeo de Protección de Datos.

Con carácter general, en todo proceso de certificación intervienen tres partes claramente diferenciadas que son:

- El organismo que elabora las normas técnicas que determinan los requisitos específicos de la certificación (esquema de certificación).
- La entidad u organismo de certificación que es la que emite el documento oficial que demuestra el cumplimiento de las normas técnicas.
- La entidad o persona certificada.

Además, los organismos de certificación expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de que, si no se cumplen o dejan de cumplirse los requisitos para la certificación, la AEPD pueda retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida o que no se emita una certificación.

Estos organismos de certificación para poder expedir, renovar o retirar certificaciones deben tener un nivel adecuado de pericia y por ello el RGPD establece que los estados miembros deben garantizar que estos organismos sean acreditados por la autoridad de control o por el organismo nacional de acreditación designado con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos, por la autoridad de control competente (AEPD).

En este sentido, la acreditación se configura como una herramienta establecida a escala internacional para generar confianza sobre la correcta ejecución de un determinado tipo de actividades que se denominan actividades de evaluación de la conformidad, en general cualquier actividad que tenga por objeto evaluar si un producto, servicio, sistema o persona es conforme con ciertos requisitos.

Nuestro organismo nacional de acreditación según la norma citada es la Entidad Nacional de Acreditación (ENAC), asociación sin ánimo de lucro, declarada de utilidad pública que fue designada por el Gobierno para operar en España como el único Organismo Nacional de Acreditación, por tanto, es el organismo nacional de acreditación. Su estructura y principios de funcionamiento garantizan que todas sus actuaciones se basan en los principios de imparcialidad, independencia y transparencia, contando en sus órganos de gobierno con todas las partes interesadas en el proceso (los acreditados, la industria usuaria de sus servicios y las administraciones públicas).

Sobre los organismos de certificación, el RGPD establece que únicamente serán acreditados si se cumplen los siguientes supuestos:

- Que hayan demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto de la certificación.
- Si se han comprometido a expedir la certificación sobre la base de los criterios aprobados por la autoridad de control.
- Si han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificación, sellos y marcas de protección de datos.
- Han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público.
- Han demostrado, a satisfacción de la autoridad de control, que sus funciones y cometidos no dan lugar a conflicto de intereses.

La acreditación se expedirá por un período máximo de cinco años y es renovable en las mismas condiciones siempre que el organismo de certificación cumpla los requisitos citados.

Los organismos de certificación son los responsables de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del Reglamento.

Estos organismos deben comunicar a la autoridad de control las razones de la expedición de la certificación solicitada o de su retirada.

Es un requisito el que la autoridad de control haga públicos en una forma fácilmente accesible los criterios aprobados para acreditar a los organismos de certificación, además las autoridades de control deben comunicar dichos criterios al Comité quien archivará en un registro todos los mecanismos de certificación y sellos de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

La autoridad de control o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación si las condiciones de la acreditación no se cumplen o han dejado de cumplirse o bien si la actuación de dicho organismo infringe el RGPD.

Es de señalar que en la Ley Orgánica 3/2018 se considera una infracción grave la utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado, así como obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del RGPD.

Finalmente señalar que la Ley Orgánica 3/2018 ha incluido en su artículo 39 la siguiente referencia al mecanismo de certificación (art. 39): “Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos

57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación”.

### 3.2. ESPECIAL CONSIDERACIÓN A LA CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS

Como se ha expuesto hasta ahora, el RGPD insta a las autoridades de control a promover la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento del mismo.

No obstante, la norma también recoge otra posible certificación, la del delegado de protección de datos, relacionada con la forma de acreditar los conocimientos del delegado de protección de datos en la materia en consonancia con lo señalado en el artículo 35 de la Ley Orgánica 3/2018 como uno de los mecanismos voluntarios para acreditar dichos conocimientos especializados.



De esta forma, la AEPD, en colaboración con la Entidad Nacional de Acreditación (ENAC), ha puesto en marcha un proceso para certificar, de forma voluntaria a Delegados de Protección de Datos, con la finalidad de ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a aquellas empresas y entes que vayan a incorporar la figura del Delegado en sus organizaciones, que sirva para acreditar su cualificación y capacidad profesional.

Para su elaboración se ha contado con la participación de un Comité Técnico de Expertos de 23 miembros, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas.

En este sentido, y teniendo en cuenta las partes que intervienen en el mismo y atendiendo con carácter general a los requisitos expuestos anteriormente, ha quedado configurado de la siguiente manera:

- El organismo propietario del esquema de certificación es la Agencia Española de Protección de Datos apoyada y asesorada por un Comité Técnico representado por aquellas asociaciones sectoriales cuyos asociados están obligados a nombrar un delegado de protección de datos, así como entidades que ya cuentan con un certificado de profesionales de la privacidad además de representantes de las universidades.
- ENAC, encargada de que las entidades de certificación cumplan los requisitos necesarios para acreditarse como tales.
- Las entidades de certificación son las que emiten el documento oficial que certifica que el Delegado de Protección de Datos cumple con los requisitos exigidos por el Esquema de Certificación, dispone de los conocimientos necesarios y está en disposición de ejercer sus funciones como tal profesional.

Cualquier entidad que desee ser certificadora del Esquema deben solicitar a ENAC la acreditación para lo cual deben pasar un proceso regulado por la normativa correspondiente y una vez superado el mismo, ENAC emitirá la correspondiente acreditación que será supervisada por la AEPD.

El propósito del esquema de certificación es establecer las normas y el procedimiento a seguir por aquellas personas o profesionales que quieran certificarse como delegados de protección de datos. En el mismo se incluyen los prerequisites que debe reunir con carácter previo a presentarse al examen que, una vez superado, le permitirá conseguir el certificado, así como el temario que debe conocer para superar el citado examen.

En el Esquema también se incluye toda aquella información, requisitos y procedimiento exigidos a las entidades de certificación para poder otorgar, suspender o retirar certificados.

Indicar que la página web de la AEPD contiene un apartado específico dedicado al Esquema de Certificación:

<https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf>

## 4. TRANSFERENCIAS INTERNACIONALES DE DATOS

### 4.1. MARCO GENERAL DE LAS TRANSFERENCIAS

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales<sup>16</sup>.

Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales<sup>17</sup>.

Como principio general para la transferencia internacional, el RGPD, en su artículo 44, establece que “Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.”

Sin embargo, dado que el RGPD no incluye una definición de transferencia internacional de datos quizás resulte adecuado, a efectos de claridad didáctica y con carácter general, tener de referencia la definición que se incluía en el artículo 5.1.s) del Reglamento de desarrollo de la antigua LOPD:

*“tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español”.*

<sup>16</sup> RGPD- Considerando 6

<sup>17</sup> RGPD-Considerando 101

Por tanto, siguiendo con el esquema propuesto en el RLOPD, cuando la transmisión de los datos tenga por destino algún Estado del EEE (UE más Noruega, Islandia y Liechtenstein), no se produce una transferencia internacional de datos desde la perspectiva jurídica. Sólo cuando su transmisión se produce fuera del Espacio Económico Europeo, ya sea con destino a otro responsable del tratamiento, que va a decidir sobre la finalidad, el contenido y uso del tratamiento, o a un encargado del tratamiento, que los tratará por cuenta del responsable, se estaría ante una transferencia internacional de datos.

Por otra parte, desde finales del año 2015 las transferencias internacionales de datos de carácter personal han tenido una relevancia pública tras las revelaciones incluidas en el denominado caso Snowden y, sobre todo, con la sentencia del Tribunal de Justicia de la Unión Europea, que invalidó la Decisión de Puerto Seguro de la Comisión Europea que consideraba que las entidades de Estados Unidos adheridas a dicho sistema adoptado por la Comisión europea en el año 2000 proporcionaban un nivel adecuado de protección, y que dio lugar a que muchos responsables de ficheros adquirieran conciencia de que estaban realizando transferencias internacionales con motivo de la contratación de determinados servicios, fundamentalmente de cloud computing.

El Puerto Seguro fue sustituido por el denominado acuerdo del Escudo de Privacidad (Privacy Shield) como sistema de garantías para poder transmitir datos a aquellas entidades establecidas en los Estados Unidos de América que hayan optado por adherirse al sistema de garantías para las transferencias internacionales incluidas en dicho marco.

Posteriormente, en julio de 2020 el Tribunal de Justicia de la Unión Europea anuló la Decisión 2016/1250 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad (Privacy Shield) para las transferencias internacionales de datos a EEUU.

La sentencia, cuyas implicaciones marcan un nuevo punto de inflexión sobre la forma en la que se realizan las transferencias internacionales de datos a EEUU, establece, a su vez, la validez de las cláusulas contractuales estándar adoptadas por la Comisión Europea para realizar transferencias internacionales de datos entre un responsable establecido en la Unión Europea y un encargado del tratamiento fuera de la UE.

En este sentido es preciso tener en cuenta que en la actualidad nos encontramos en una situación compleja como consecuencia de la citada sentencia ya que dicho marco de adecuación quedó invalidado y, aunque, como ya se ha señalado, las denominadas cláusulas contractuales tipo, junto con el resto de instrumentos como las reglas corporativas vinculantes, fueron declaradas válidas, el TJUE obliga a tomar una serie de medidas suplementarias con el fin de que la legislación aplicable en países terceros, en concreto, en Estados Unidos, proporcione un nivel de protección sustancialmente equivalente.

Hasta ahora, en el marco del Comité Europeo de Protección de Datos, se han adoptado una serie de documentos encaminados a que los exportadores e importadores de datos puedan realizar una evaluación con el fin de determinar que el nivel de protección es sustancialmente equivalente al que ofrecen las herramientas de transferencia en el marco del Espacio Económico Europeo.

En el siguiente enlace se encuentran disponibles las FAQ elaboradas por el Comité Europeo de protección de datos al respecto:

<https://www.aepd.es/sites/default/files/2020-08/faqs-sentencia-SCHREMS-II-es.pdf>

Con respecto a las novedades que el RGPD establece en la regulación de las transferencias internacionales de datos, es preciso señalar que parte de los criterios ya establecidos en la Directiva 95/46 e incorporados en nuestra legislación interna, es decir, que sólo se podrán transmitir datos a aquellos países, territorios, sectores u organismos internacionales respecto de los que la Comisión Europea haya considerado que disponen de un nivel adecuado o equivalente de protección, o, en otro caso, se aporten garantías suficientes o se den algunas de las circunstancias previstas como excepciones, y siempre y cuando se observen los demás requisitos del mencionado RGPD.

No obstante, el RGPD introduce novedades que afectan a todo el régimen de transferencias internacionales, pero vamos a fijarnos en las que hacen referencia al régimen de autorizaciones que supone un cambio radical con respecto al modelo desarrollado en el marco de la Directiva 95/46 y la normativa nacional aplicable.

La primera cuestión a destacar es que el RGPD establece sin duda alguna que el exportador de datos puede ser tanto un responsable como un encargado del tratamiento, precisión con la que definitivamente se pone fin a las restricciones legales de determinados Estados miembros en los que el exportador ha de ser siempre el responsable del tratamiento, lo que da lugar a que los prestadores de servicio establecidos en terceros países se encuentren en mejor situación a la hora de subcontratar en esos u otros terceros países que los prestadores de servicios establecidos en la UE. Esta situación fue abordada por la AEPD mediante la adopción de las cláusulas contractuales que permitían regular las transferencias internacionales entre un encargado establecido en España y subencargados en terceros países.

Así mismo, se amplía el abanico de instrumentos en los que se pueden incluir y aportar las garantías adecuadas para proteger los derechos de los afectados como consecuencia de la transferencia de datos. Así, se incorporan los códigos de conducta y los mecanismos de certificación como instrumentos que pueden aportar esas garantías, además de las Normas Corporativas Vinculantes (conocidas por sus siglas en inglés, BCR-Binding Corporate Rules) para los grupos multinacionales que, aunque en la práctica ya están operativas, merced al trabajo desarrollado en el seno del Grupo del artículo 29, por primera vez se reconocen con rango legal, lo que va a posibilitar su uso en aquellos Estados miembros que hasta la fecha no las consideran válidas al derivarse su carácter vinculante no sólo de la vía contractual sino también de declaraciones unilaterales. Esta gama más amplia de instrumentos tendría que facilitar la labor de los exportadores al disponer de un mayor abanico de instrumentos entre los que elegir.

Pero donde más evidente son las novedades que introduce el RGPD es en el régimen de autorización y notificación previa de las transferencias internacionales, que quedan reducidas a muy pocos supuestos.

La normativa aplicable en España hasta el 25 de mayo de 2018 obligaba a los exportadores de datos a solicitar una autorización previa para poder transferir datos a importadores establecidos en países que no cuentan con un nivel adecuado de protección, siempre que aporten las garantías suficientes, y a notificar las transferencias cuando se dirigen a países que sí disponen de dicho nivel adecuado o, en otro caso, se realizan al amparo de alguna de las excepciones previstas en la LOPD.

Sin embargo, en el marco del RGPD, con carácter general, las transferencias se pueden llevar a cabo sin necesidad de autorización previa, salvo que las garantías se aporten a través de un contrato entre el responsable o el encargado del tratamiento, encargado o destinatario de los datos personales en el tercer país u organización internacional, o de un acuerdo administrativo entre autoridades públicas, supuestos

en los que será preciso que exista la autorización de la autoridad de control, tal y como señala el artículo 46.3 del RGPD.

## 4.2. TRANSFERENCIAS BASADAS EN UNA DECISIÓN DE ADECUACIÓN

El RGPD señala en su Considerando 102 que “...Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados”.

Hasta la fecha la Comisión Europea ha considerado países que ofrecen un nivel adecuado de protección a los siguientes países y territorios:

- Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón y Reino Unido.
- Canadá (sólo cuando a la entidad destinataria le sea de aplicación la “Personal Information and Electronic Documents Act”).

## 4.3. TRANSFERENCIAS MEDIANTE GARANTÍAS ADECUADAS

En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente<sup>18</sup>.

Así en el artículo 46 se relacionan las garantías adecuadas que podrán ser aportadas sin que se requiera ninguna autorización expresa de una autoridad de control:

<sup>18</sup> RGPD- Considerando 108



- un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- normas corporativas vinculantes (BCR);
- cláusulas tipo de protección de datos adoptadas por la Comisión;
- cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;
- un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados;
- un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

Por su parte, la AEPD contribuyó a facilitar la tarea de aportar garantías, mediante la elaboración en 2012 de un conjunto de cláusulas estándar, sobre la base de las establecidas por la Comisión en su Decisión 2010/87/UE, para las transferencias internacionales realizadas entre un encargado del tratamiento como exportador y un subencargado importador de los datos.

Las garantías se establecen en favor de los interesados, de ahí que las cláusulas sean exigibles no sólo por los firmantes del contrato, sino también por los interesados, en particular cuando sean perjudicados por el incumplimiento del contrato. Por ello, todos los modelos contienen una cláusula, denominada de tercero beneficiario, por la que los interesados pueden exigir el cumplimiento del contrato aun no siendo parte de él.

Sin embargo, estas cláusulas de encargado subencargado aprobadas por la AEPD no podrán utilizarse en el contexto del RGPD como cláusulas tipo de protección de datos mientras no sean adoptadas por la Comisión.

#### 4.4. NORMAS CORPORATIVAS VINCULANTES

El RGPD señala, en su Considerando 110, en relación con las denominada Normas corporativas vinculantes (más conocidas por sus siglas en inglés BCR –Binding Corporate Rules-) que “Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal”.

En este sentido, en el RGPD se definen las normas corporativas vinculantes como “las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta”. (Artículo 4 apartado 20).

Para su aprobación por la autoridad de control competente, el RGPD establece una serie de requisitos que se han plasmado en diversos documentos elaborados, en su momento, por el denominado Grupo del

Artículo 29 de la Directiva 95/46<sup>19</sup>. Posteriormente algunos de estos documentos han sido revisados para su adaptación al RGPD<sup>20</sup>.

Estos requisitos se enumeran en el artículo 47 del RGPD:

- sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;
- confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales; y
- cumplan e incluyan, como mínimo los siguientes requisitos y elementos:
  - a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;
  - b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;
  - c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;
  - d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;
  - e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;
  - f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;
  - g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14 relativos a la información que debe facilitarse a los interesados;
  - h) las funciones de todo delegado de protección de datos designado, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas

<sup>19</sup> WP 74, WP 107, WP 108, WP 133, WP 153, WP 155, WP 195 y WP 204

<sup>20</sup> WP 263.rev.01 – Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR; WP 264

vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

- i) los procedimientos de reclamación;
- j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;
- k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;
- l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);
- m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y
- n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

#### 4.5. EXCEPCIONES PARA SITUACIONES ESPECÍFICAS

Adicionalmente, tal y como ya figuraba en la Directiva 95/46 y en la normativa española de protección de datos, se consideran una serie de excepciones a los supuestos generales para la transferencia internacional de datos.

Así se indica en el Considerando 111 del RGPD que “Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de

dichas personas o, si estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado”.

Y según el Considerando 112: “Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso de contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados”.

Dado que se consideran excepciones al régimen general, el RGPD, como ya lo hizo el Grupo del artículo 29 en su documento WP 114<sup>21</sup>, quiere clarificar el régimen restrictivo del uso de dichas excepciones, por lo que conforme al Considerando 113: “Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sea aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado”.

Así, la Ley Orgánica 3/2018 señala como supuesto que deberá ser previamente comunicado a la autoridad de protección de datos competente cuando la transferencia internacional se pretenda llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos del responsable, así como a los afectados por la transferencia (art. 43).

Como supuestos sometidos a autorización previa de las autoridades de protección de datos (art. 42 Ley Orgánica 3/2018) se encuentran las transferencias internacionales de datos a países u organizaciones

<sup>21</sup> WP 114 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. Puede consultarse en la siguiente dirección: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm)

internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo 41 de la Ley Orgánica 3/2018 y en el artículo 46.2 del RGPD. Estas requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo aprobadas por la Comisión europea o cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de la ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

Estas autorizaciones quedarán sometidas a la emisión por el Comité Europeo de Protección de Datos del dictamen en el marco del mecanismo de coherencia.