EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Módulo 5.Las autoridades de supervisión. El Comité Europeo de Protección de Datos. El régimen sancionador en el RGPD.

MINISTERIO
DE HACIENDA
Y ADMINISTRACIONES PÚBLICAS

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

Contenido

5.1.- LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

5.1.1. NATURALEZA JURÍDICA.

El artículo 51 del Reglamento General de Protección de Datos (RGPD) estipula que cada Estado miembro establecerá que una, o varias, autoridades públicas independientes (denominadas autoridades de control) supervisen su aplicación con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la UE. Previsión que ya contenía la Directiva 95/46, precedente del RGPD, en su artículo 28, en el que se subrayaba que dichas autoridades ejercerán las funciones que le son atribuidas con total independencia.

La Agencia Española de Protección de Datos (AEPD) es la **autoridad de control independiente** que vela por el cumplimiento de la legislación en materia de protección de datos. En desarrollo del artículo 28 de la Directiva, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) establece que *"la Agencia Española de Protección de Datos (AEPD) es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones"*, y se rige por lo dispuesto en la propia LOPD y en su Estatuto, aprobado por el Real Decreto 428/1993, en desarrollo de la primera Ley de Protección de Datos, conocida como la LORTAD.

Además, y en virtud de la previsión contenida en el artículo 41 de la LOPD, existen las autoridades de control autonómicas que ejercen sus funciones en relación con su respectivo sector público y que son la Agencia Vasca de Protección de Datos, la Autoridad Catalana de Protección de Datos, y el Consejo de Transparencia y Protección de Datos de Andalucía, si bien esta última todavía no está operativa como autoridad de protección de datos. Por su parte, el Estatuto de la AEPD completa la descripción de su naturaleza jurídica, definiéndolo como un ente público de los previstos en la ya derogada Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (LOFAGE) que en su disposición adicional décima establece el régimen jurídico de aplicable a la AEPD. Esta disposición adicional también establece que este organismo público se regirá por su normativa específica y supletoriamente por la LOFAGE. Es importante destacar que no se le aplica en ningún caso la Ley de Agencias Estatales.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, deroga la LOFAGE, pero señala en su disposición transitoria segunda que los organismos y entidades del sector público estatal continuarán rigiéndose por su normativa específica hasta su adaptación a lo dispuesto en la Ley, para lo que se establece un plazo de 3 años desde su entrada en vigor, según dispone en la disposición adicional cuarta.

Es por ello que en el Anteproyecto de Ley Orgánica de Protección de Datos que se está tramitando, se establece que la AEPD es una autoridad administrativa independiente de ámbito estatal, de las previstas en el artículo 109 de la Ley 40/2015 como integrante del sector público institucional estatal, con plena personalidad jurídica y plena capacidad pública y privada que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones, y que se relaciona con el Gobierno a través del Ministerio de Justicia.

5.1.2. RÉGIMEN JURÍDICO APLICABLE.

La LOPD establece que la AEPD se rige por su normativa específica, en concreto por la propia LOPD y sus disposiciones de desarrollo, al que el APLOPD antepone el RGPD y señala que el Gobierno aprobará su estatuto a propuesta de la propia AEPD.

En concreto, el artículo 35 LOPD enumera el régimen jurídico de los diferentes ámbitos de actuación de la AEPD se recoge en el artículo 35 de la LOPD en los siguientes términos:

- En el ejercicio de sus funciones públicas, en aquello que no disponga la LOPD y sus normas de desarrollo, actuará de conformidad con las Leyes 39 y 40/2015, de Procedimiento Administrativo Común y de Régimen Jurídico del Sector Público.

- En materia de contratación se regirá por la Ley de Contratos del Sector Público.

- En cuanto al personal, los puestos de trabajo son desempeñados por funcionarios y por personal laboral, según la naturaleza de las funciones asignadas a cada puesto de trabajo. De acuerdo con ello, el régimen del personal que presta servicios en la AEPD será el previsto en el Estatuto Básico del Empleado Público y la normativa de función pública aplicable, cuando se trate de funcionarios públicos, y en la normativa laboral y el Convenio Único para el personal laboral de la AGE.

- La AEPD elabora su presupuesto y lo remite al Gobierno para que sea integrado con independencia en los Presupuestos Generales del Estado.

- Para el cumplimiento de sus fines dispone de las asignaciones presupuestarias los bienes valores que constituyan su patrimonio, así como los bienes y valores y cualquier otros recursos que legalmente se le atribuyan.

- En lo relativo al control de las actividades económicas y financieras de la Agencia, el control externo lo ejerce el Tribunal de Cuentas y el interno la Intervención General de la Administración del Estado.

- La contabilidad de la Agencia se ajusta al Plan General de Contabilidad Pública.

El APLOPD prácticamente reproduce el régimen este régimen jurídico en la figura de una autoridad administrativa independiente, destacando la inclusión entre los bienes y medios para el cumplimiento de fines los recursos derivados del ejercicio de sus actividades, incluida la potestad sancionadora.

5.1.3. ESTRUCTURA Y FUNCIONES.

a.- Carácter de autoridad independiente

Un aspecto capital de la AEPD es el de su independencia, tal y como se viene reconociendo en toda la normativa: la Directiva 95/46, la LOPD, el RGPD y el APLOPD.

Para ello, el RGPD estipula en su artículo 52 que el miembro o los miembros de cada autoridad de control serán ajenos en el desempeño de sus funciones y en el ejercicio de sus poderes a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna excepción. Se abstendrán de cualquier acción incompatible con sus funciones, ni participarán en actividad profesional, remunerada o no, que resulte incompatible.

b.- Estructura orgánica básica

b.1.- El Director

De conformidad con el artículo 36 de la LOPD, el Director dirige la Agencia, ostenta la representación de la misma, ejerce sus funciones con plena independencia y objetividad, desempeña su cargo con dedicación absoluta y no estará sujeto a instrucción de autoridad alguna.

Será nombrado por Real Decreto de entre los miembros del Consejo Consultivo a propuesta del Ministro de Justicia, por un periodo de cuatro años.

El cese se puede producir a petición propia, por separación en caso de incumplimiento grave, incapacidad, incompatibilidad o comisión de delito doloso y por cumplimiento de su mandato.

El RGPD añade que poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

El APLOPD, que cambia su denominación por la de Presidente y extiende su mandato a 5 años prorrogable una vez, indica que será nombrado por el Gobierno, a propuesta del Ministro de Justicia, entre profesionales de reconocida competencia con conocimientos y experiencia acreditados para el desempeño de sus funciones y, con carácter previo al nombramiento, el Congreso de los Diputados emitirá un dictamen acerca de su idoneidad.

b.2.- El Consejo Consultivo

La LOPD y el APLOPD establecen un órgano colegiado, el Consejo Consultivo, que asesora al Director/Presidente de la AEPD, emite informe sobre las cuestiones que éste

le someta y podrá formular propuestas sobre temas relacionados con las materias de competencia de la AEPD.

La composición del Consejo es la siguiente:

- Un Diputado.
- Un Senador.
- Un representante de la Administración General de del Estado, propuesto por el Ministro de Justicia.
- Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
- Un representante de cada Comunidad Autónoma con Autoridad propia de Protección de Datos. Recae en los Directores de las Agencias Autonómicas.
- Un representante de la Administración Local propuesto por la FEMP.
- Un miembro de la Real Academia de la Historia.
- Un experto en la materia, propuesto por el Consejo Superior de Universidades.
- Un representante de los usuarios y consumidores, propuesto por el Consejo de Consumidores y Usuarios.
- Un representante del sector de ficheros de titularidad privada, propuesto por el Consejo Superior de Cámaras.

El APLOPD modifica su composición al suprimir los vocales propuestos por la Real Academia de la Historia y por el Consejo Superior de Universidades, e incorporar como nuevos miembros a:

- Un representante de las entidades responsables y encargadas de los tratamientos, propuesto por las organizaciones empresariales.
- Un representante de los profesionales de la protección de datos designado por el Ministerio de Justicia.
- Un representante del Consejo General del Poder Judicial.

El actual estatuto de la AEPD establece que el Consejo Consultivo se reunirá cuando así lo decida el Director que, en todo caso, lo convocará una vez cada seis meses, o cuando así lo solicite la mayoría de sus miembros. El APLOPD establece que al menos se reunirá una vez al año.

La normativa actualmente aplicable establece una estructura basada en 3 órganos: el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, que se ve afectada por las novedades introducidas por el RGPD, como la supresión de la obligación de registrar los ficheros, y que, en consecuencia, habrá de replantearse en el estatuto de la AEPD que se acabe adoptando.

Además, la AEPD cuenta con una Unidad de Apoyo al Director, un Gabinete Jurídico, un Departamento de Relaciones Internacionales y una Unidad de Estudios y Evaluación Tecnológica.

5.1.4. FUNCIONES Y POTESTADES DE LA AEPD.

Con la finalidad de supervisar la aplicación del RGPD, éste atribuye a las autoridades de control, y por tanto a la AEPD, un elenco de funciones y de potestades en sus artículos 57 y 58, respectivamente, que conforman sus competencias y que tienen su reflejo en las funciones previstas en el artículo 37 de la LOPD.

Las funciones que el RGPD atribuye a las autoridades de control, y por tanto a la AEPD, son:

- Controlar su aplicación del RGPD y hacerlo aplicar;
- Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de datos. Debiendo prestar especial atención a las actividades dirigidas específicamente a los niños;
- Asesorar, con arreglo al Derecho interno, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;
- Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del RGPD;
- Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del RGPD y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;
- Tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;
- Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del RGPD;
- Llevar a cabo investigaciones sobre la aplicación del RGPD, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;
- Hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;
- Adoptar las cláusulas contractuales tipo para los encargados del tratamiento y las transferencias internacionales de datos;
- Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos;
- Ofrecer asesoramiento sobre las operaciones de tratamiento de datos personales en los casos en los que una evaluación de impacto muestre que el

tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo;
- Alentar la elaboración de códigos de conducta y dictaminar y aprobar los códigos de conducta de ámbito nacional que den suficientes garantías;
- 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;
- Elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta y de organismos de certificación;
- Efectuar la acreditación de organismos de supervisión de los códigos de conducta y de organismos de certificación;
- Autorizar las cláusulas contractuales presentadas en contratos "ad hoc" y en disposiciones incorporadas a acuerdos administrativos entre autoridades y organismos públicos que incluyan las garantías adecuadas para realizar transferencias internacionales de datos;
- Aprobar normas corporativas vinculantes;
- Contribuir a las actividades del Comité Europeo de Protección de Datos;
- Llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas en el ejercicio de los poderes correctivos, y
- Cualquier otra función relacionada con la protección de los datos personales.

Por su parte, y para el ejercicio de las referidas funciones, el artículo 58 del RGPD atribuye a las Autoridades de control los siguientes poderes o atribuciones:

- **Poderes de investigación:**

  - Ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;
  - Llevar a cabo investigaciones en forma de auditorías de protección de datos;
  - Llevar a cabo una revisión de las certificaciones;
  - Notificar al responsable o al encargado del tratamiento las presuntas infracciones del RGPD;
  - Obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;
  - Obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

- **Poderes correctivos:**

- Sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el RGPD;
- Sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RGPD;
- Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del RGPD;
- Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado;
- Ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales;
- Retirar una certificación u ordenar al organismo de certificación que retire una certificación o que no se emita si no se cumplen o dejan de cumplirse los requisitos para la certificación;
- Imponer una multa administrativa, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
- Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

- **Poderes de autorización y consultivos:**

  - Asesorar al responsable del tratamiento conforme al procedimiento de consulta previa sobre las operaciones de tratamiento de datos personales en los casos en los que una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo;
  - Emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho interno, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;
  - Autorizar con carácter previo el tratamiento de datos realizado por un responsable en el ejercicio de una misión realizada en interés público, en

particular el tratamiento en relación con la protección social y la salud pública, siempre que se determine en el Derecho nacional;
- Emitir un dictamen y aprobar proyectos de códigos de conducta;
- Acreditar los organismos de certificación;
- Expedir certificaciones y aprobar criterios de certificación;
- Autorizar cláusulas las transferencias internacionales basadas en cláusulas contractuales "ad hoc" y en disposiciones incorporadas a acuerdos administrativos entre autoridades y organismos públicos;
- Autorizar los acuerdos administrativos para las transferencias internacionales de datos entre autoridades y organismos públicos;
- Aprobar normas corporativas vinculantes.

En el ejercicio de las funciones de inspección atribuidas a la AEPD, los funcionarios que la desempeñen tienen la consideración de autoridad pública, según se estipula en la LOPD y también en el APLOPD.

Además, elaborará un informe anual de sus actividades que se remitirá al Parlamento nacional, al Gobierno y a aquellas autoridades que establezca la normativa interna, que ya se recoge en la normativa actualmente aplicable.

Por su parte, el APLOPD atribuye las siguientes potestades a la AEPD:

- Dictar las disposiciones de desarrollo y ejecución necesarias para la interpretación y cumplimiento de lo dispuesto en el RGPD.
- El ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos. Le corresponde a la AEPD la representación común de las autoridades autonómicas de protección de datos en el Comité Europeo de Protección de Datos, en el que cada Estados miembro estará representado por una autoridad de control.
- Así mismo, coordinará la misión de dictámenes del Comité Europeo de Protección de Datos cuando se refieran a proyectos que deban someterles las Agencias autonómicas, y en las reclamaciones que les afecten.
- La convocatoria, por medio de su presidente, de las Agencias autonómicas de protección de datos con carácter regular para contribuir a la aplicación coherente del RGPD.

5.1.5. RECLAMACIONES ANTE LA AEPD.

La Directiva 95/46 recoge que toda autoridad de control entenderá de las solicitudes que cualquier persona le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales.

El RGPD estipula que todo interesado, sin perjuicio de cualquier otro recurso administrativo o acción judicial, tendrá derecho a presentar una reclamación ante una

autoridad de control si considera que el tratamiento de datos personales que le conciernen infringen el RGPD, y, como se ha señalado, entre las funciones que atribuye a las autoridades de control está la de tramitar las reclamaciones presentadas por un interesado o por un organismo e investigar en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

La LOPD, referido a los derechos de acceso, rectificación, cancelación y oposición, establece que las actuaciones contrarias a la Ley pueden ser objeto de reclamación por los interesados ante la AEPD, lo que se traduce en los procedimientos de tutela de dichos derechos cuando no son atendidos por los responsables del tratamiento. No obstante, debemos incluir también en este ámbito cualquier reclamación que, como hemos visto, se considere que afecta al derecho a la protección de datos de los interesados.

El Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007 de 21 de diciembre (RLOPD), establece los procedimientos para la tramitación de las reclamaciones, ya se trate de tutelas de derecho o de procedimientos relativos al ejercicio de la potestad sancionadora. Las reclamaciones por tutela de derechos se han de formular por los propios interesados o por quien debidamente los represente y se han de resolver en un plazo máximo de seis meses por el procedimiento establecido en el RLOPD.

En el supuesto de reclamaciones que dieran lugar a un procedimiento sancionador se pueden realizar actuaciones previas encaminadas a determinar la concurrencia de motivos que lo justifiquen que no podrán extenderse más de 12 meses. Iniciado el procedimiento sancionador tendrá una duración máxima de 6 meses.

EL APLOPD recoge que las reclamaciones tramitadas por la AEPD se rigen por lo dispuesto en el RGPD, por lo que disponga la Ley, por las disposiciones reglamentarias, que regulará el Gobierno mediante Real Decreto asegurando en todo caso los derechos de defensa y de audiencia de los interesados, y con carácter subsidiario por la normas generales sobre los procedimientos administrativos.

La AEPD, de conformidad con lo dispuesto en el RGPD, determinará con carácter previo a la iniciación de un procedimiento el carácter nacional o transfronterizo, o remitirá la reclamación formulada a la Autoridad de control principal que se considere competente.

En todo caso, se inadmitirán las reclamaciones que no versen sobre cuestiones de protección de datos, carezcan de fundamento, sean abusivas o no se aporten elementos que permitan investigar la existencia de vulneración de los derechos reconocidos.

Un aspecto novedoso que introduce el APLOPD es la intervención del Delegado de Protección de Datos (DPD) en casos de reclamaciones ante la AEPD, al habilitar la posibilidad de que el afectado se dirija con carácter previo a la presentación de la reclamación ante la AEPD al Delegado de Protección de Datos, que tendrá un plazo máximo de 2 meses para adoptar la decisión. Si el afectado presentase la reclamación ante la AEPD si haberla planteado ante el Delegado de Protección de Datos, aquélla podrá remitir la reclamación al Delegado de Protección de Datos (DPD) para que resuelva en el plazo de 1 mes. Transcurrido dicho plazo sin que se comunique a la AEPD la decisión adoptada, ésta continuará con el procedimiento.

En el mismo sentido, cuando el responsable o encargado del tratamiento contra el que se dirija la reclamación esté adherido a un código de conducta que hubiera establecido procedimientos extrajudiciales o de mediación de los conflictos en materia de protección de datos, la AEPD podrá remitir al organismo establecido la reclamación para que le dé respuesta, y tramitarla en el caso de que se rechazase.

Los plazos para la tramitación de los procedimientos, que no podrán superar los 18 meses, quedarán automáticamente suspendidos cuando deba recabarse información, consulta o pronunciamiento de un órgano de la UE o de una Autoridad de control conforme establece el RGPD hasta la notificación del pronunciamiento a la AEPD.

Antes de la iniciación del procedimiento la AEPD podrá incoar actuaciones previas a fin de determinar la concurrencia de circunstancias que lo justifiquen, que no podrán superar el plazo de 1 año que se suspenderá en los mismos supuestos indicados en el párrafo anterior.

Las resoluciones que pongan fin a los procedimientos de reclamación serán objeto de publicación.

Establece el RGPD que toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante que le concierna de una autoridad de control, por lo que las resoluciones de la AEPD agotan la vía administrativa, por lo que pueden ser objeto de recurso de reposición, ante la propia AEPD, y ante la jurisdicción de la Sala de lo Contencioso Administrativo de la Audiencia Nacional.

5.2. EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS.

5.2.1.- NATURALEZA Y COMPOSICIÓN.

El Comité Europeo de Protección de Datos (CEPD) es el órgano encargado de velar por la aplicación coherente del Reglamento General de Protección de Datos (RGPD).

El Comité es el sucesor del Grupo de Trabajo del Artículo 29 (GT29, que agrupa a las Autoridades europeas de protección de datos) previsto en la Directiva 95/46, pero existen diferencias sustanciales entre ambos.

A diferencia del GT29, el Comité adopta la forma de organismo de la Unión, y tiene personalidad jurídica propia.

Su composición es también similar a la del GT29. Está formado por el director o presidente de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos (SEPD), o sus representantes respectivos.

La posición del SEPD es peculiar. En principio, es miembro de pleno derecho y como tal puede participar como cualquier otro miembro en los trabajos del Comité.

Sin embargo, hay una diferencia clara entre el SEPD y los demás miembros del Comité:

- Las Instituciones, agencias y organismos de la Unión no se rigen por el RGPD, sino por su propio Reglamento de Protección de Datos. En la actualidad ese Reglamento es el 45/2001, aunque está siendo revisado, justamente para adaptarlo al RGPD. Consecuentemente, el SEPD, como Institución de la Unión, no está sometido al RGPD ni tampoco lo aplica en su tarea de supervisión.

  Por todo ello, aunque el SEPD puede participar como cualquier otra autoridad en el CEPD, en el caso de las decisiones que se adopten en virtud del artículo 65 del RGPD, a las que más adelante nos referiremos, sólo podrá votar en decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que se correspondan en cuanto al fondo a las contempladas en el RGPD.

Por otra parte, cuando en un Estado Miembro haya varias autoridades encargadas de controlar la aplicación del RGPD, se nombrará a una de ellas miembro representante común, siempre de acuerdo con el derecho nacional de cada Estado.

Esta previsión del RGPD está pensada, fundamentalmente, para atender a situaciones como la de España, donde aparte de la Agencia Española existen varias autoridades autonómicas, con competencias referidas al sector público de sus respectivas Comunidades. Es también el caso de Alemania, donde hay autoridades de control distintas de la autoridad federal en cada uno de los estados federados.

En España, el representante común de todas las autoridades de control es la Agencia Española de Protección de Datos. El texto de la futura Ley Orgánica de Protección de Datos (APLOPD) que sustituirá a la actualmente vigente, incluye disposiciones relativas al modo en que se articulará la participación de las autoridades autonómicas en las actividades del CEPD.

Por su parte, la Comisión Europea no es, realmente, miembro del Comité. Tiene derecho a participar en sus reuniones y actividades, pero sin voto. Para ello, deberá designar a un representante y deberá ser informada por el Presidente del CEPD sobre las actividades del Comité.

El CEPD actuará con total independencia en el ejercicio de sus funciones y no podrá recibir instrucciones de ningún tipo. El único caso en que tiene que atender las

indicaciones de otra Institución de la Unión es el de las peticiones de informe de la Comisión, sobre las que tiene la obligación de responder y, en su caso, hacerlo en los plazos que fije la Comisión.

5.2.2. FUNCIONAMIENTO.

El Comité cuenta con un Presidente y dos Vicepresidentes, que serán elegidos por mayoría simple de entre sus miembros. El mandato del Presidente y de los Vicepresidentes será de cinco años, y podrá renovarse una sola vez.

El Presidente convoca las reuniones del Comité, notifica sus decisiones y es el encargado de velar por el buen funcionamiento de los trabajos del Comité. Aunque el RGPD no se pronuncia sobre ello, es de suponer que el Presidente, como sucede ahora con el GT29, asuma también la función de representación del CEPD.

Esta cuestión, como otras relacionadas con el funcionamiento del CEPD, podrá incluirse en el Reglamento de Régimen Interior que el CEPD deberá aprobar. Este Reglamento está siendo preparado por el GT29 y será sometido a la aprobación del CEPD, que deberá pronunciarse sobre él por mayoría de dos tercios de sus miembros, tan pronto como se constituya formalmente en 2018.

El CEPD tendrá una Secretaría, que será asumida por el Supervisor Europeo de Protección de Datos (SEPD). Dicho en otros términos, el CEPD no cuenta con personal ni presupuesto propios, sino que éstos le serán proporcionados por el SEPD.

Las funciones de la Secretaría incluyen todo lo relacionado con la gestión necesaria para que el CEPD pueda desempeñar su labor (gestión presupuestaria, organización de reuniones, interpretación y traducción,…) pero también la preparación, redacción y publicación de dictámenes, decisiones relativas a la solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Esto puede dar lugar a conflictos de intereses, dado que el SEPD es, a la vez, miembro del CEPD y se ocupa de prestar servicios de Secretaría que pueden tener influencia en el contenido de las decisiones que adopte el Comité.

Para evitar esos posibles conflictos, el personal del SEPD que participe en los trabajos de Secretaría dependerá de un superior jerárquico distinto del que se ocupe de las funciones propias del SEPD.

Además, el SEPD y el CEPD suscribirán un memorando de entendimiento en el que se establecerán los términos de la cooperación entre ambos y también las obligaciones del personal vinculado a la Secretaría.

5.2.3. FUNCIONES.

Es en las funciones que el RGPD atribuye al CEPD donde más claramente se perciben las diferencias con el GT29, pudiendo agruparse las mismas en tres categorías, diferenciadas por los efectos de las decisiones que el Comité puede adoptar.

- **Funciones consultivas, de asesoramiento y guía.**

Estas funciones constituyen el núcleo principal del artículo 70 del RGPD.

Es en este artículo donde se prevé, por ejemplo, que el CEPD asesorará a la Comisión en cualquier materia en que ésta le consulte.

La mayoría de las funciones recogidas en este artículo tienen que ver con la adopción de recomendaciones, directrices o buenas prácticas en una gran cantidad de materias. Entre ellas pueden citarse las decisiones automatizadas basadas en perfiles, la identificación de violaciones de seguridad y los criterios para notificar a las autoridades de control o a los interesados, la aplicación de las medidas correctivas y multas previstas en el RGPD o los criterios para realizar transferencias internacionales sobre la base de las excepciones previstas en el artículo 49.1 del RGPD.

También aquí se encomienda al CEPD el promover la cooperación entre sus miembros, a través, entre otros, de programas de formación comunes e intercambios de documentación y personal.

Estas funciones son las que más se asemejan a las que actualmente tiene atribuidas el GT29. Sin embargo, las diferencias cuantitativas y cualitativas son muy notables, lo que contribuye a subrayar el papel central que el CEPD tiene atribuido en el sistema de protección definido por el RGPD.

Por un lado, mientras que las funciones del GT29 se resumen en la Directiva en apenas cinco apartados de un artículo, formulados de una manera genérica, las del Comité se desarrollan a lo largo de veintisiete apartados del mencionado artículo 70.

Estos apartados están redactados, además, de forma muy precisa, indicando específicamente tanto el aspecto de cada materia sobre el que actuará el CEPD como la misión concreta que se le encomienda.

Ello permite suponer que, aunque las directrices, recomendaciones o dictámenes que el Comité adopte en aplicación de este artículo no sean jurídicamente vinculantes, están llamadas a tener un peso determinante en la interpretación y aplicación del RGPD, en la medida en que procederán de un órgano al que el RGPD le confiere expresamente y en exclusividad esas funciones, sin perjuicio de las competencias que corresponden a la Comisión y a los tribunales.

- **Funciones de autorización.**

Estas funciones se recogen en el artículo 64 del RGPD, dentro del capítulo dedicado al llamado "mecanismo de coherencia".

El mecanismo de coherencia, en el que se integran tanto los dictámenes que se adopten en aplicación de este artículo 64 como las decisiones derivadas del artículo 65, que se tratará más adelante, es una de las principales novedades del RGPD.

Se configura como un instrumento específicamente diseñado para permitir al CEPD alcanzar el objetivo de lograr la aplicación coherente del RGPD.

En ambos artículos, con las diferencias que a continuación se detallan, se pretende dotar al Comité de competencias reforzadas para asegurar que las decisiones que adopte cada autoridad de control en los Estados Miembro sigan criterios comunes y consistentes en todas las materias que puedan tener efectos en el conjunto de la Unión.

En el caso del artículo 64, las autoridades nacionales están obligadas a someter al dictamen del Comité las decisiones que tengan previsto adoptar en los siguientes ámbitos:

- Listas de tratamientos que deben ser objeto de evaluación de impacto sobre la protección de datos
- Aprobación de códigos de conducta que afecten a varios Estados Miembro
- Aprobación de criterios para la acreditación de organismos de supervisión de códigos de conducta o de organismos de certificación
- Modelos de clausulado para contratos de encargo de tratamiento
- Cláusulas contractuales tipo para transferencias internacionales adoptadas por una autoridad nacional
- Cláusulas contractuales "ad hoc" presentadas por un exportador para ofrecer garantías en una transferencia internacional de datos
- Normas corporativas vinculantes

Esta lista permite ver con más claridad cuál es el objeto de estos dictámenes. Lo que se persigue es controlar que si una autoridad de un Estado Miembro decide, por ejemplo, autorizar las normas corporativas vinculantes que le haya presentado una empresa multinacional, la decisión no se aleja de las valoraciones, criterios o interpretaciones comunes que haya ido estableciendo el Comité.

En suma, se trata de avanzar un paso más desde las recomendaciones o directrices previstas en el artículo 70 hace el objetivo de lograr que el RGPD se aplica uniformemente en toda la Unión. Visto desde otra perspectiva, supone que ninguna autoridad de control nacional podrá tomar decisiones unilateralmente sin tener en cuenta la opinión del Comité.

Esta competencia del Comité no se limita a esta lista de materias tasadas. Cualquier autoridad de control, el Presidente del Comité o la Comisión podrán pedir al Comité que emita un dictamen sobre asuntos de interés general o que afecten a más de un Estado Miembro.

El Comité deberá emitir dictamen, por mayoría simple de sus miembros, en un plazo de ocho semanas desde que reciba la propuesta de decisión, siempre que no se hubiera pronunciado ya sobre el asunto con anterioridad, en cuyo caso podrá declinar la adopción del dictamen.

La autoridad de control que haya presentado la propuesta de decisión no podrá adoptarla mientras se sustancia el procedimiento ante el Comité.

El RGPD prevé que el Presidente circule entre los miembros toda la información pertinente por medios electrónicos.

El RGPD parece apuntar a un procedimiento de adopción de los dictámenes basado en la aceptación, en principio, de las propuestas, salvo que alguno de los miembros plantee objeciones dentro de los plazos marcados por el Presidente en cada caso.

Los dictámenes del Comité en virtud del artículo 64 no tienen carácter jurídicamente vinculante en sí mismos. Pero ello no significa que carezcan de importantes efectos para las autoridades implicadas.

En primer lugar, el RGPD establece que la autoridad que haya propuesto la decisión "tendrá en cuenta en la mayor medida posible" el contenido del dictamen del CEPD. En el plazo de dos semanas desde que reciba la notificación del dictamen deberá

comunicar al Presidente si piensa modificar su decisión siguiendo los contenidos del dictamen, cuando este sea el caso, y enviar el proyecto de decisión modificada.

Más relevante aún es el hecho de que si la autoridad de control decide desoír en todo o en parte el dictamen del Comité, se aplicará el mecanismo de resolución de conflictos del artículo 65, que se trata en el siguiente apartado. Ello supone que un dictamen que no es vinculante en sí mismo puede tener esos efectos si la autoridad afectada no lo respeta y si así lo decide el Comité.

- **Funciones de resolución de conflictos.**

Estas funciones se recogen en el artículo 65 del RGPD y son las que mejor definen el nuevo papel que corresponde al CEPD.

En síntesis, el artículo 65 prevé que el Comité podrá adoptar decisiones jurídicamente vinculantes para las autoridades que lo integran en tres supuestos concretos. Todos ellos se refieren a situaciones en que dos o más autoridades discrepan entre sí en la aplicación del RGPD en materias que tienen efectos en más de un Estado Miembro.

Uno de estos supuestos ya se ha mencionado en el apartado anterior. Se trata de los casos en que una autoridad de control no solicite el dictamen del Comité estando obligada a ello o en que no siga el dictamen del Comité. Según el artículo 65.1.c del RGPD, cualquier autoridad afectada o la Comisión pondrán el asunto en conocimiento del CEPD.

Los otros dos supuestos que recoge el artículo 64 tienen que ver con el mecanismo de cooperación para la adopción de decisiones que afectan a tratamientos de datos transfronterizos.

A los efectos de analizar las funciones del CEPD, bastará aquí con señalar que **se consideran tratamientos transfronterizos aquellos que lleva a cabo un responsable (o encargado) en el contexto de las actividades de varios establecimientos en varios Estados Miembro. Tendrán también esa consideración los tratamientos que, aunque se lleven a cabo en el contexto de las actividades de uno o varios establecimientos en un solo Estado Miembro, afectan significativamente a personas en varios Estados Miembro.**

Un ejemplo de este tipo de tratamientos sería el de las grandes empresas prestadoras de servicios de la sociedad de la información, que tienen establecimientos en prácticamente todos los Estados Miembro de la Unión. También serían tratamientos transfronterizos los que desarrolle, por ejemplo, una página de comercio electrónico instalada solo en un Estado Miembro pero que ofrece sus productos a consumidores en varios Estados Miembro, con webs en diferentes idiomas y ofertas específicamente diseñadas para cada Estado.

Lo relevante para considerar un tratamiento como transfronterizo es que haya establecimientos en dos o más Estados o que estén afectados ciudadanos en dos o más Estados. Cuestiones como que las posibles reclamaciones contra el tratamiento se hayan presentado en varios Estados Miembros o solo en uno de ellos, o que la empresa sea de origen europeo o proceda de un país tercero son irrelevantes a estos efectos.

En estos tratamientos, la gestión de las reclamaciones de los interesados o de las investigaciones que puedan desarrollarse ante posibles infracciones del RGPD es coordinada por una autoridad que tiene la consideración de "autoridad principal". Las autoridades de los demás Estados en que la empresa tenga establecimientos o en los que residan interesados "significativamente afectados" participarán también en el procedimiento como "autoridades afectadas".

Esa autoridad es la del Estado Miembro donde el responsable tiene su establecimiento principal.

El RGPD establece que se considerará establecimiento principal la administración central de la compañía en la Unión, salvo que sea otro establecimiento en la Unión el que tome las decisiones sobre los fines y medios del tratamiento transfronterizo de que se trate.

Simplificando mucho el sistema, podría ponerse el siguiente ejemplo:

Un banco multinacional español, con sucursales o filiales en varios Estados Miembro, las cuales tratan los datos de sus clientes siguiendo los criterios establecidos por la central en España y empleando programas y aplicaciones desarrollados en la central.

En ese supuesto, la Agencia Española sería la autoridad principal ante cualquier reclamación que pudiera plantear un interesado contra el banco y las autoridades de los Estados Miembro donde haya sucursales o filiales serían autoridades afectadas.

- **Un primer problema** es el de establecer dónde está el establecimiento principal. La definición del RGPD puede ser fácil de aplicar en determinadas organizaciones, pero puede plantear problemas en otras que estén estructuradas de forma compleja, con entramados de sociedades en varios Estados Miembro que desempeñen varios papeles de diferente naturaleza en relación con los procesos de tratamiento de datos. Por ejemplo, un banco puede desarrollar también un negocio de seguros a través de una empresa del grupo y puede darse la circunstancia de que las sedes principales del negocio bancario y de la actividad aseguradora se encuentren en diferentes Estados Miembro. La determinación de cuál es el establecimiento principal si, por ejemplo, ambas empresas comparten una parte de sus clientes y también determinados procesos para el tratamiento de sus datos, personales puede resultar compleja.

- **El segundo supuesto** en que el RGPD atribuye al Comité la facultad de resolver conflictos entre las autoridades de control se refiere, precisamente, a esos casos en los que no hay acuerdo entre las autoridades implicadas sobre dónde se sitúa el establecimiento principal y, consiguientemente, cuál de ellas es la autoridad principal.

  Siguiendo con el mecanismo de coherencia, su idea central es que las decisiones sean adoptadas de común acuerdo por todas las "autoridades afectadas", por mucho que sea la autoridad principal la que dirija el procedimiento y que le corresponda a ella elaborar las propuestas de decisión.

- **El último y tercer supuesto**, previsto en el artículo 65 del RGPD, cuando no se logre el acuerdo porque una o varias "autoridades afectadas" discrepen de la propuesta de la autoridad principal y ésta decida mantener su propuesta, el asunto será remitido al CEPD para que se pronuncie sobre las objeciones planteadas por las autoridades discrepantes.

En los tres casos el CEPD adoptará decisiones vinculantes para sus miembros en el plazo de un mes, prorrogable por otro mes si el tema es especialmente complejo, por mayoría de dos tercios de sus miembros.

No obstante, si en esos plazos el Comité no ha logrado alcanzar la mayoría requerida, la decisión podrá adoptarse por mayoría simple dentro de las dos semanas siguientes a la finalización del segundo mes.

Estas decisiones del CEPD deben ser cumplidas por las autoridades a las que concierne en el plazo de un mes desde que les sean notificadas. Las decisiones de las autoridades nacionales que apliquen las del Comité deberán hacer referencia a estas últimas y especificar que son publicadas en la web del CEPD.

Las decisiones del Comité en virtud del artículo 65 pueden ser recurridas por cualquiera de los miembros del Comité ante el Tribunal de Justicia de la Unión Europea.

También pueden ser objeto de recurso directo ante el Tribunal por parte de los afectados por los procedimientos que dieron lugar a que el Comité debiera pronunciarse. Estos últimos podrán recurrir indirectamente la decisión del CEPD ante los tribunales nacionales cuando planteen recursos contra las decisiones de las autoridades que apliquen las del Comité. En este último caso, si se cuestiona indirectamente la decisión del CEPD en el recurso nacional, los tribunales nacionales deberán plantear una cuestión prejudicial ante el Tribunal de Justicia de la UE, ya que éste es el único que puede anular una decisión de un organismo de la Unión.

5.3. El régimen sancionador en el RGPD.

5.3.1. Introducción.

El capítulo VIII del RGPD, bajo el título "Recursos, responsabilidad y sanciones", regula el régimen sancionador aplicable, que debe ser completado con lo que al respecto regule la nueva Ley Orgánica de Protección de Datos, ya que el RGPD no realiza una regulación detallada al respecto. Así, por ejemplo, el RGPD no contempla lo referente a la prescripción de infracciones, tan característica en el régimen sancionador español de

cualquier materia, ni tampoco realiza una clasificación de las infracciones en leves, graves y muy graves.

Esta circunstancia es debida a que este sistema de sanciones o actuaciones correctivas es sumamente genérico, en el que no se tipifican las conductas ni se establecen las reacciones concretas ante su comisión, la nueva Ley Orgánica de Protección de Datos (Anteproyecto de Ley Orgánica de Protección de Datos) que se está tramitando, procede a describir las conductas típicas, manteniendo la distinción entre infracciones muy graves, graves y leves, a la vista de la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. Puesto que la categorización de las infracciones afecta también a sus plazos de prescripción, esta nueva ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del RGPD.

En este sentido, el citado Anteproyecto considera como sujetos sometidos al régimen sancionador del RGPD y de la citada Ley Orgánica a los siguientes:

a) Los responsables de tratamiento.
b) Los encargados de los tratamientos.
c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta.

5.3.2. Infracciones y sanciones.

En primer lugar, debemos tener en consideración el artículo 83, apartados 1 y 2, del RGPD, que señala lo siguiente:

- Las multas administrativas (poder correctivo contemplado en el artículo 58.2.i del RGPD) serán efectivas, proporcionadas y disuasorias.

- Se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58.2 en donde se relacionan los poderes correctivos que disponen las Autoridades de Control.

Asimismo, y al objeto de graduar la cuantía de las sanciones pecuniarias, el mencionado artículo 83.2, establece los siguientes **criterios de graduación**:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32; e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Además, este precepto se completaría con lo que al respecto prevé el **Anteproyecto de Ley Orgánica de Protección de Datos** que se está tramitando, cuyo artículo 76.2, atendiendo a que el apartado k) del artículo 83.2 del RGPD se refiere a "cualquier otro factor agravante o atenuante (…)", **prevé como criterios de graduación de las sanciones**:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

Por otra parte, los apartados 4, 5 y 6 del artículo 83, se refieren a los límites de la cuantía de las sanciones pecuniarias en función de la infracción cometida:

- Artículo 83.4:señala una multa de cuantía máxima de 10.000.000 €, o el 2% del volumen de negocio total (optándose por la de mayor cuantía entre ambos valores) en la comisión de las siguientes infracciones :

    a) Las obligaciones del responsable y del encargado a tenor de los artículos:

        - Artículo 8 ("consentimiento de los menores").
        - Artículo 11 ("tratamientos que no requieren identificación").
        - Artículos 25 a 39:
            - ✓ *Artículo 25 "protección de datos desde el diseño y por defecto".*
            - ✓ *Artículo 26"corresponsables del tratamiento".*
            - ✓ *Artículo 27 "representantes de responsables o encargados no establecidos en la Unión".*
            - ✓ *Artículo 28 "encargado del tratamiento"*
            - ✓ *Artículo 29 "tratamiento bajo la autoridad del responsable o del encargado del tratamiento".*
            - ✓ *Artículo 30 "registro de actividades del tratamiento".*
            - ✓ *Artículo 31 "cooperación con la autoridad de control".*
            - ✓ *Artículo 32 "seguridad del tratamiento".*
            - ✓ *Artículos 33 y 34 "notificación y comunicación de violaciones de seguridad".*
            - ✓ *Artículo 35 "evaluación relativa a la protección de datos".*
            - ✓ *Artículo 36 "consulta previa".*
            - ✓ *Artículos 37 a 39 "delegado de protección de datos".*

    b) Las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

    c) Las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

- El artículo 83.5 señala una multa de cuantía máxima de 20.000.000 €, o el 4% del volumen de negocio total (optándose por la de mayor cuantía entre ambos valores) en la comisión de las siguientes infracciones :

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX:

art.85 Tratamiento y libertad de expresión y de información.

art.86 Tratamiento y acceso público a documentos oficiales.

art.87 Tratamiento del número nacional de identificación.

art.88 Tratamiento en el ámbito laboral.

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

El artículo 83.6 señala una multa de cuantía máxima de 20.000.000 €, o el 4% del volumen de negocio total (optándose por la de mayor cuantía entre ambos valores) en la comisión de la infracción por incumplimiento de las resoluciones de la Autoridad de Control a tenor de lo dispuesto en el artículo 58.2.

Además, las sanciones que se impongan pueden ser a título adicional (o sustitutivo) entre las contempladas en el artículo 58.2, en el caso de incumplimiento de diversas disposiciones el artículo 83.3 limita la cuantía total de la multa a la prevista para las infracciones más graves, que no son otras que las dispuestas en el artículo 83.5 y 6.

Asimismo, y en función de lo dispuesto en el artículo 83 apartados 4 y 5, el Anteproyecto de Ley Orgánica de Protección de Datos que se está tramitando, recoge todo un catálogo de infracciones leves, graves y muy graves.

INFRACCIONES MUY GRAVES		
Tratar datos personales vulnerando los principios y garantías del art. 5 del RGPD.	Tratar datos personales sin que concurran alguna de las condiciones de licitud del art. 6 del RGPD.	Incumplimiento requisitos del art. 7 del RGPD para la validez del consentimiento.
Uso de datos para finalidad no compatible para la que fueron recabados, sin contar consentimiento del afectado o base legal para ello.	Tratamiento de datos del art.9 del RGPD sin concurrir circunstancias de dicho precepto o del art.10 de esta ley.	Tratamiento datos de condenas e infracciones penales o medidas de seguridad fuera de lo dispuesto en el 10 del RGPD o 20 de esta ley.
Tratamiento de datos de infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 4.	Omisión del deber de informar conforme a lo dispuesto en los arts. 13 y 14 del RGPD y 21 de esta ley.	Vulneración del deber de confidencialidad del artículo 6 de esta ley.
Exigencia de pago de canon para facilitar la información que se refiere en los arts. 13 y 14 del RGPD.	No atender las solicitudes de derechos de los arts. 15 a 22 del RGPD fuera de los supuestos establecidos en su art. 12.5	Impedimento/obstaculización/no atención reiterada del ejercicio de derechos de los arts. 15 a 22 del RGPD.

Transferencia internacional de datos a destinatario de tercer país u organización internacional, sin las garantías de los arts. 44 a 49 del RGPD.	Incumplimiento de resoluciones dictadas por la autoridad de control en ejercicio de los poderes del 58.2 del RGPD.	Incumplimiento de la obligación de bloqueo del art.29 de esta ley cuando la misma sea exigible
Resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos.	No facilitar el acceso del personal de la autoridad de control a los datos personales, información, locales, equipos o medios de tratamiento que sean requeridos en el ejercicio de sus poderes de investigación.	

INFRACCIONES GRAVES		
Tratamiento de datos de menor de 13 años sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela.	No acreditar esfuerzos razonables para verificar la validez del consentimiento prestado por menor de 13 años o titular de su patria potestad o tutela.	Incumplimiento por un organismo de certificación de los principios y deberes a los que está sometido conforme a los arts. 42 y 43 del RGPD.
Falta de adopción de medidas técnicas y organizativas apropiadas para aplicar la privacidad desde el diseño y por defecto e integrar garantías necesarias en el tratamiento.	Falta de adopción de medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo se traten datos necesarios para cada fin, conforme al 25.2 del RGPD.	Incumplimiento de designar representante del responsable o encargado no establecido en la UE, conforme al 27 del RGPD.
Falta de atención de representante en la UE del responsable o encargado de las solicitudes efectuadas por la autoridad de protección de datos o los afectados.	Contratación por el responsable de un encargado que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas del capítulo IV del RGPD.	Contratación por un encargado de otros encargados sin contar la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.
Encargar tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido del 28.3 RGPD.	Infracción por un encargado de lo dispuesto en el RGPD y esta ley, al determinar los fines y medios del tratamiento, conforme al 28.10 del RGPD.	No poner a disposición de la autoridad de control que lo haya solicitado el registro de actividades de tratamiento
No disponer del registro de actividades de tratamiento del art.30 del RGPD.	No cooperar con la autoridad de control en el desempeño de sus funciones en los supuestos no previstos del art.72 de esta ley.	Tratamiento de datos sin previa valoración de los riesgos que pudiera generar a los derechos de los afectados, y en particular a su protección de datos, conforme al art.30 del RGPD.
Incumplimiento del deber del encargado de notificar al responsable las violaciones de seguridad.	Incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad, conforme al art. 33 del RGPD.	El tratamiento de datos sin realizar evaluación de impacto en los supuestos que sea exigible.
Incumplimiento del deber de comunicar al afectado una violación de seguridad conforme al art.34 del RGPD, si el responsable hubiese sido requerido por la autoridad de protección de datos para realizarlo.	Tratamiento de datos sin haber consultado previamente a la autoridad de control cuando sea preceptiva conforme al art.36 del RGPD o una ley establezca la obligación de realizarla.	Incumplimiento de obligación de designar delegado de protección de datos cuando sea exigible su nombramiento conforme al art.37 del RGPD.
No posibilitar la participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos, no respaldarlo o interferir en sus funciones.	Uso de un sello o certificación de protección de datos que no haya sido otorgado por una entidad de certificación acreditada o en caso de que la vigencia del mismo hubiera expirado.	Obtener acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos del art. 43 del RGPD.
Desempeño de funciones que el RGPD reserva a los organismo de certificación, sin haber sido acreditado conforme al art.40 de esta ley.	Desempeño de funciones que el art.41 del RGPD reserva a los organismos de certificación de supervisión de códigos de conducta sin haber sido acreditado por la autoridad de control.	Falta de adopción por los organismos acreditados de supervisión de un código de conducta de las medidas oportunas en caso de infracción del código, conforme al art.41.4 del RGPD.
Impedimento/obstaculización/no atención reitera de derechos de acceso, rectificación, supresión, limitación al tratamiento u portabilidad en tratamientos que no requieran identificación del afectado, cuando éste, haya facilitado información adicional que permita la identificación.		

INFRACCIONES LEVES		
Incumplimiento del principio de transparencia de la información/derecho de información por no facilitar todo lo exigido conforme arts. 13 y 14 RGPD.	No atender las solicitudes de ejercicio de derechos de los arts.15 a 22 del RGPD, salvo que sea de aplicación 72.1.k) de esta ley.	Incumplimiento obligación informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se han comunicado los datos rectificados, suprimidos o limitado tratamiento.
Incumplimiento obligación de notificar la rectificación/supresión/limitación de datos exigida por el 19 RGPD.	Incumplimiento de suprimir los datos referidos a una persona fallecida cuando sea exigible conforme al art.3 de esta ley.	No poner a disposición de los afectados los aspectos esenciales del acuerdo entre corresponsables del tratamiento, conforme al 26.2 RGPD.
No atender derechos acceso, rectificación, supresión, limitación del tratamiento o portabilidad que no se requiera identificación del afectado, cuando éste haya facilitado información adicional que permita su identificación, salvo que se aplicase el art.73.c) de esta ley.	Falta de formalización por los corresponsables del tratamiento del acuerdo sobre obligaciones, funciones y responsabilidades y sus relaciones con los afectados, conforme al 26.2 del RGPD.	Falta del cumplimiento de la obligación del encargado de informar al responsable acerca de posible infracción por una instrucción recibida de éste de las disposiciones del RGPD o de esta ley, conforme al 28.3 del RGPD.
Incumplimiento por encargado o subencargado del contrato o acto que regule el tratamiento o instrucciones del responsable, salvo que esté legalmente obligado conforme el RPGD y esta ley o supuesto que fuese necesario para evitar infracción y se hubiese advertido al responsable o al encargado.	Exigencia del pago de un canon al afectado para facilitar información exigida por arts.13 y 14 del RGPD o por atender las solicitudes de derechos de los arts.15 a 22 del RGPD cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes para facilitar la información o realizar la actuación solicitada.	Incumplimiento por los organismos acreditados de supervisar un código de conducta de la obligación de informar a las autoridades de control sobre las medidas en caso de infracción del código, conforme al art. 41.4 del RGPD.
Disponer un registro de actividades del tratamiento que no incorpore toda la información del art.30 del RGPD.	Incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el 33.5 del RGPD.	Facilitar información inexacta a la autoridad de control, en los supuestos de consulta previa, conforme al 36 del RGPD.
Notificación incompleta o defectuosa a la autoridad de control de la información sobre una violación de seguridad conforme al art.33 del RGPD.	No publicar datos de contacto del delegado de protección de datos, cuando su nombramiento sea exigible conforme al 37 del RGPD y 35.3 de esta ley.	Incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de control de la expedición, renovación o retirada de una certificación, conforme al art.43.1 y 43.5 del RGPD.
Incumplimiento del deber de comunicar al afectado una violación de seguridad que entrañe alto riesgo para derechos y libertades, conforme al 34 del RGPD, salvo que sea de aplicación el art. 73.q) de esta ley.		

Respecto a la prescripción, el Anteproyecto de Ley Orgánica recoge tanto la prescripción de infracciones y sanciones, como la interrupción del plazo de prescripción de las infracciones de la siguiente forma:

- **Prescripción de infracciones:**
  - Leves, graves y muy graves, prescriben al año, dos años y tres años respectivamente.
- **Interrupción de prescripción de infracciones:**
  - La iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de un año por causas no imputables al presunto infractor.

- Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del RGPD interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas.

- **Prescripción de sanciones:**

  - Las que sean de importe inferior a los 40.000 euros prescriben en el plazo de un año; de 40.001 a 300.000 euros a los dos años; y las que superen los 300.000 euros a los tres años.

- **Cómputo y prescripción de sanciones:**

  - Este plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

  - La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Por último, y a título de curiosidad, el artículo 83.9 hace mención a dos países de la Unión, Dinamarca y Estonia, toda vez que sus ordenamientos jurídicos internos no permiten el establecimiento de multas administrativas, por lo que regula que la incoación de la multa corresponde a la Autoridad de Control y su imposición a los tribunales nacionales competentes.

5.3.2. Poderes correctivos de la Autoridad de Control.

Anteriormente, en el apartado de este módulo referente la funciones y potestades que confiere el RGPD a las autoridad de control, y por ende a la Agencia Española de Protección de Datos, ya nos referimos a los poderes que confiere al respecto el artículo 58 del RGPD y que son de investigación (art 58.1), correctivos (art 58.2) y de autorización y consultivos (art 58.3).

No obstante, el ejercicio de estos poderes estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

Además, el RGPD contempla en el apartado 6 del citado artículo 58 que cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicados.

Respecto a los poderes correctivos del artículo 58.2 del RGPD, aunque ya se han citado en este módulo, conviene recordarlos realizando una serie de matizaciones en algunos de sus apartados.

Estos poderes correctivos, que se pueden disponer a título adicional o sustitutivo, son los siguientes:

a) Sancionar a todo responsable o encargado del tratamiento con una **Advertencia** cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento; (ver Considerando 131).

En cuanto a la Advertencia, no debe considerarse un poder correctivo de tipo sancionador, toda vez que se limita - con anterioridad a quedar acreditada una determinada infracción - a notificar al responsable o encargado la posibilidad que de seguir en su conducta podría incurrir en infracción así como recomendar el cese de un supuesto tratamiento que podría devenir en infracción. Se debe añadir que la norma no limita el número de Advertencias que se puedan notificar a un mismo responsable.

Según el Anteproyecto de Ley Orgánica de Protección de Datos:

No procederá la iniciación del procedimiento sancionador, aun cuando se hubiere formulado reclamación, en los casos en que el encargado o responsable del tratamiento, previa advertencia formulada por una Autoridad de Control, haya adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos, siempre que no se haya causado perjuicio al afectado y/o que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas impuestas.

Por último, y a efectos meramente didácticos, es plausible que la futura doctrina armonizada de las diferentes Autoridades de Control haga uso de la **Advertencia** sólo en aquellos casos en los que la posible infracción de la que trae causa pueda responder a infracciones de carácter meramente formal entre las dispuestas en el artículo 83.4 y 5 del RGPD.

b) Sancionar a todo responsable o encargado del tratamiento con **Apercibimiento** cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento.

Sobre este apercibimiento, el considerando 148 del RGPD especifica lo siguiente:

A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada

para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

En la resolución de Apercibimiento se establecerán las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. Al igual que en el caso de la Advertencia, el RGPD no limita el número de Apercibimientos a un responsable o encargado del tratamiento.

La todavía vigente LOPD regula también esta figura del apercibimiento, si bien de forma diferente al RGPD. Así, según el artículo 45.6 de la LOPD:

Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

- *Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.*

- *Que el infractor no hubiese sido sancionado o apercibido con anterioridad.*

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

Añade el Considerando 152 del RGPD:

En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

5.3.3. El régimen sancionador para las Administraciones públicas.

Respecto a la imposición de multas a las Administraciones públicas, el artículo 83.7 del RGPD señala lo siguiente:

Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

La actual la normativa al respecto se encuentra regulada en el artículo 46 de la todavía vigente LOPD y 129 del RLOPD. La LOPD determina que cuando las infracciones fueren cometidas en ficheros de titularidad pública, la AEPD dictará resolución declarando la infracción con las medidas que proceda adoptar para que cesen los efectos de la infracción así como podrá proponer la actuación de medidas disciplinarias. Asimismo, comunicará al Defensor del Pueblo la resolución y las actuaciones correctivas llevas a cabo por el responsable.

En este sentido, el Anteproyecto de Ley Orgánica de Protección de Datos prevé al respecto lo siguiente en su artículo 77:

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.
3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos podrá proponer también la iniciación de actuaciones disciplinarias. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.
6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones en que se imponga una sanción a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Es decir, la previsión es adoptar un sistema similar al que regula la vigente LOPD, no sancionando con multas pecuniarias a las Administraciones públicas que infrinjan la normativa de protección de datos, sino utilizar la vía del apercibimiento que hemos analizado anteriormente.