uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

***Coordinadora Curso:* -Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 2: PROTECCIÓN DE DATOS: RÉGIMEN GENERAL

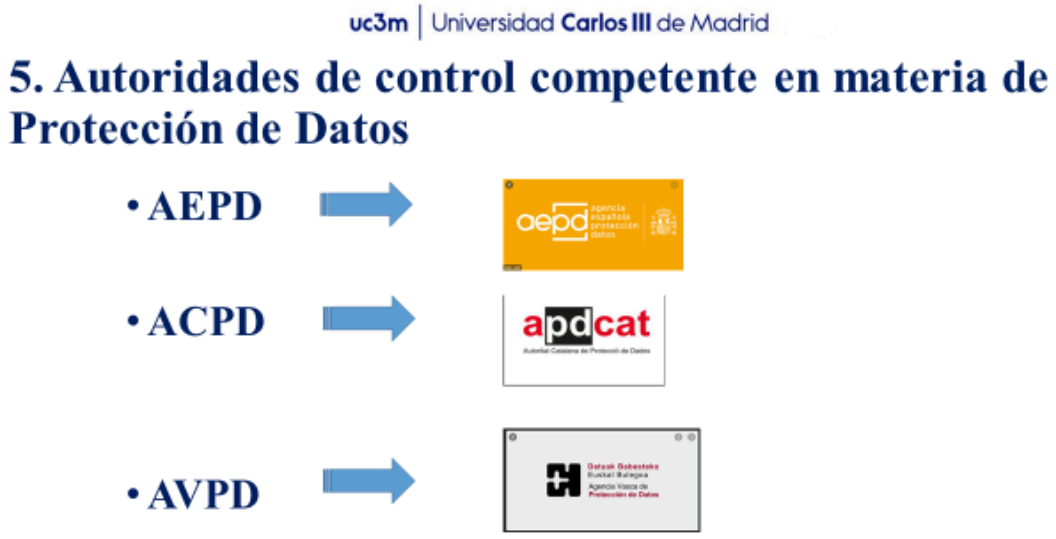
V. SUJETOS

Elaborado por PhD. Mª NIEVES DE LA SERNA BILBAO
Profesora Titular de Derecho Administrativo// Departamento de Derecho Público
Codirectora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid

SUMARIO:

V. SUJETOS

1. Autoridades de control competente en materia de Protección de Datos



El RGPD permite que existan una o varias autoridades públicas de control independientes[1] con la función de supervisar la aplicación del reglamento para conseguir una aplicación coherente, proteger los derechos y libertades de las personas físicas respecto del tratamiento de los datos y facilitar la libre circulación de los datos personales en la Unión. Corresponde a los Estados miembros su concreción pero el RGPD reconoce numerosas funciones menos, salvo el control del tratamiento de datos efectuados por los tribunales en el ejercicio de su función judicial que se lo atribuye a otro órgano[2]. También el RGPD les reconoce diversas potestades administrativas como las de

[1] Respecto del concepto de independencia véase los artículos 52 y 53 RGPD
[2] Artículos 55.3 y 57 RGPD

investigación, correctivas, de autorización y consultivas a la que pueden sumarse otras que los Estados miembros consideren[3].

La LOPDGDD desarrolla aquellos mandatos en el Título VII que contiene el régimen de la Agencia Española de Protección de Datos (en adelante, AEPD) y regula la existencia de las autoridades autonómicas de protección de datos y la obligación de actuar entre ellas cooperando y prestándose asistencia mutua en el marco del mecanismo de coherencia[4]. Recordemos que actualmente existe en España la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos[5]. La AEPD se configura como una autoridad administrativa independiente, que se relaciona con el Gobierno a través del Ministerio de Justicia[6]. Su estatuto se contiene en el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la AEPD y la misma actúa sujeta al Derecho administrativo tanto en el ejercicio de sus competencias como en el de su régimen patrimonial y de contratación[7].

Ante la AEPD y las autoridades autonómicas, se puede presentar solicitudes y reclamaciones siempre que se considere que el tratamiento de los datos no se ha efectuado cumpliendo la normativa de protección de datos. Corresponde a aquellas autoridades adoptar las medidas correspondientes para facilitar la presentación de reclamaciones y solicitudes así como investigar y resolver, dentro de su ámbito competencial, las solicitudes presentadas[8]. La LOPDGDD

[3] Artículo 58 RGPD
[4] Véase al respecto los artículos 60 y ss RGPD
[5] Véase al respecto la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos y el Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos y Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos y el Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.
[6] Con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
[7] Para más información https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/marco-normativo
[8] Artículo 77 RGPD

regula en el Título VIII, el Procedimiento administrativo que debe seguirse ante la AEPD en caso de vulneración de la normativa de protección de datos.
Finalmente destacar que es obligatorio que todas las resoluciones adoptadas por las autoridades de control nacionales de protección de datos jurídicamente vinculantes para los interesados, para los responsables o para los encargados de tratamiento, se deben poder recurrir ante los órganos jurisdiccionales del propio Estado miembro. En otras palabras, se debe tener derecho a la tutela judicial efectiva[9]. La LOPDGDD establece en el artículo 48.6 que: *"Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional."*

2.- Sujetos que intervienen en materia de protección de datos

2.1 Presentación

Todos los sujetos que intervienen en el tratamiento de los datos se encuentra identificados y definidos por el RGPD. Para todos ellos concreta un verdadero estatuto jurídico al atribuirles, a lo largo del articulado, importantes derechos y obligaciones. Estos sujetos pueden ser personas físicas o jurídicas, públicas o privadas, y cada uno cuenta con un estatuto propio y específico, y con un régimen sancionador en caso de incumplimiento. Veamos cada uno de ellos.

[9] Artículos 78 y ss RGPD

2.2 El «responsable del tratamiento» o «responsable»

El **«responsable del tratamiento» o «responsable»** se define en el RGPD como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"*[10].

Se trata, por tanto, del sujeto que define los fines y los medios del tratamiento. En el caso que un responsable del tratamiento tenga diversos establecimientos en más de un Estado miembro, el establecimiento principal será el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal[11].

Las responsabilidades de este sujeto son diversas y se articulan a lo largo del RGPD. Particular interés tiene el Título V referido a las obligaciones de los responsables del Tratamiento. Se regula aquí el principio de responsabilidad proactiva, en los términos previstos por los artículos 24 y 25 del RGPD, que implica que los responsables del tratamiento habrán de determinar las medidas técnicas y organizativas apropiadas que aplicarán en el tratamiento a fin de garantizar y acreditar su conformidad con el reglamento de la Unión, con la propia LOPDGDD, con sus normas de desarrollo y con la legislación sectorial que resulte aplicable. Todo ello, teniendo en cuenta siempre los mayores riesgos que podrían producirse en los supuestos que se recogen en el apartado

[10] Artículo 4 RGPD
[11] Artículo 4 RGPD

segundo del artículo 28 de la LOPDGDD. El siguiente artículo prevé la posibilidad de aplicación en ciertos casos de un régimen de corresponsabilidad en el tratamiento.

Se debe destacar que al responsable no sólo se le exige la adopción de medidas que persigan el cumplimiento de las obligaciones sino, también, la obtención de resultado. Así, por ejemplo, el RGPD dispone *"Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas"*[12].

Así, el artículo 5.2 RGPD señala respecto del cumplimiento de los principios por parte del responsable que su obligación no sólo se centra en cumplir con los mismos sino, también, en ser "*capaz de demostrarlo* («responsabilidad proactiva»)". Igual consideración merece lo dispuesto en el artículo 8.2 RGPD cuando concreta las obligaciones respecto del consentimiento de los niños en relación con los servicios de la sociedad de la información, en donde se exige a los responsables que realice *"esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.*

Finalmente, el RGPD concreta un importante régimen sancionador que se modulará o agravará según sea su conducta. El artículo 83 RGPD y siguientes recogen diversas sanciones que comprenden multas administrativas de 10.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del

[12] Considerando 74 RGPD

ejercicio financiero anterior, a multas de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

2.3 El «encargado del tratamiento» o «encargado»

Otro sujeto relevante en esta materia es el **«encargado del tratamiento» o «encargado»,** que se define como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento"*[13]. Se trata de un sujeto que depende del responsable. Éste es quien lo selecciona y responde, en principio, por sus actos, por lo debe elegir al que le ofrezca las garantías suficientes de aplicar el RGPD. La forma y el tipo de relación que se concrete entre ambos sujetos dependerá siempre de la clase de servicios que vaya a prestarle al responsable. En todo caso, el RGPD obliga a que esta relación se formalice un contrato u otro acto jurídico similar con un contenido concreto[14].

Como señala el propio RGPD *"Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a*

[13] Artículo 4 RGPD
[14] Téngase presente las *"Directrices para la elaboración de contratos entre responsables y encargados del tratamiento"* de la AEPD, de fecha 16 de mayo de 2018

un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos"[15]. Los artículos 28 y ss del RGPD articulan el régimen aplicable a estos sujetos.

Finalmente señalar que si un encargado del tratamiento cuenta con establecimientos en más de un Estado miembro, su establecimiento principal será el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento[16].

[15] Considerando 81 y artículos 28 y ss RGPD
[16] Artículo 4 RGPD

2.4 El «representante»

Cuando el responsable o el encargado del tratamiento se encuentren radicados fuera de la Unión Europea, la empresa obligatoriamente debe designar por escrito a un **representante** establecido en uno de los Estados miembros en los que se encuentren los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado[17]. Los "representantes" se definen en el RGPD como "*las persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento*[18].

2.5 El «Delegado de Protección de Datos –DPD-»

Por último, el RGPD articula una figura nueva, un participante clave en el nuevo sistema de gestión de los datos, el **Delegado de Protección de Datos –DPD- o Data Protection Officer -DPO-**. Se establecen las condiciones para su nombramiento, su puesto y sus tareas[19]. Concretamente el artículo 39 RGPD realiza una relación de funciones mínimas y el artículo 37 señala que tanto el responsable como el encargado del tratamiento de datos deben designar un

[17] Artículo 4 y 27 RGPD
[18] Véase al respecto el artículo 27 RGPD
[19] Véase al respecto las Directrices sobre los delegados de protección de datos (DPD) adoptadas el 5 de abril de 2017, (WP 243 rev.01) por el Grupo de Trabajo del artículo 29.

Delegado de protección de Datos siempre que se den los supuestos que señala que son:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) 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

c) 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 DPD debe ser designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho, la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el RGPD[20]. Igualmente, se permite que este sujeto pueda formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios y resulta obligatorio publicar los datos de contacto de éste, así como comunicar los mismos a la autoridad de control. También está obligado a mantener el secreto y la confidencialidad en lo que respecta al desempeño de sus funciones.

Es importante destacar que el delegado no puede recibir instrucciones para el desempeño de sus funciones, ni del responsable ni del encargado, debe actuar con total independencia. Tampoco este sujeto puede ser destituido ni sancionado por éstos sujetos, pero aquellos deben respaldar al delegado en el desempeño de estas funciones y para ello deben facilitarle los recursos necesarios para el desempeño de aquellas así como el acceso a los datos

[20] En particular lo dispuesto en el artículo 39 RGPD

personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados[21].

Finalmente, los interesados pueden contactar con el delegado para todas las cuestiones relativas a protección de datos y el mismo estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

Al DPD se le permite desempeñar otras funciones y cometidos, siempre que se garantice que dichas funciones y cometidos no den lugar a conflicto de intereses.

3.- Responsabilidad proactiva –*Accountability*-

Una de las novedades más importantes del RGPD, es la inclusión del principio de responsabilidad proactiva que obliga al responsable, no sólo a cumplir con los principios que recoge el RGPD, sino también, que debe ser capaz de demostrar su cumplimiento. Este principio se encuentra recogido en el artículo 5 del RGPD en los siguientes términos *"El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)."*

El principio mencionado se encuentra desarrollado en el artículo 24.1 RGPD y artículo 28 LOPDGDD. El primero de ellos señala textualmente *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que*

[21] Artículo 38 RGPD

el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."

Por su parte, el artículo 32 del RGPD establece que las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se deben definir en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

De lo anterior se deduce que el RGPD no establece medidas de seguridad estáticas y será al responsable a quien le corresponda determinar aquellas que resulten necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Es así que un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos. Para garantizar la confidencialidad, la integridad y la disponibilidad de los datos se deben por tanto adoptar alguna de las medidas, de índole técnica y de índole organizativa que recoge el RGPD y que son:

a) Neutralidad tecnológica y Privacidad desde el diseño (PbD) y por defecto[22]

b) Evaluación de Impacto (EIPD)[23]

c) Adopción de medidas de seguridad adecuadas[24]

d) Llevar un Registro de Actividades de Tratamiento (RAT)[25]

e) Notificación de las brechas de seguridad[26]

4.- Régimen sancionador

[22] Considerando 15 y artículo 25
[23] Artículos 35 RGPD y 28 LOPDGDD
[24] Artículo 32 RGPD
[25] Artículos 30 RGPD y 31 LOPDGDD
[26] Artículos 4.12 y 33 y 34 RGPD

El régimen sancionador se recoge en el RGPD, concretamente en el Capítulo VIII, bajo el título "Recursos, responsabilidades y sanciones". En comparación con el régimen anterior, el RGPD viene a endurecer considerablemente las sanciones y se señala que se fijarán en función del tipo de obligación que se incumpla. El artículo 83 RGPD señala al respecto que la autoridad de control garantiza que las multas administrativas sean efectivas, proporcionadas y disuasorias y que se pondrán en función de las circunstancias de cada caso individual. Las Autoridades también tienen potestades correctivas que serán adicionales a la imposición de multas administrativas[27] y un amplio margen de apreciación para la determinación de la cuantía de las sanciones concretando factores agravantes y atenuantes –artículos 83- que se deben tener en cuenta para fijar la sanción. Es así que para determinar el nivel y el tipo de la sanción impuesta se debe considerar la naturaleza, la gravedad y la duración de la infracción; la existencia de culpa o de dolo; las medidas que adoptadas para mitigar los daños; la cooperación con la Autoridad de Control; la proactividad en la notificación de los hechos causantes de los daños; las categorías de datos personales afectadas, entre otros[28].

El RGPD señala que se deben imponer las siguientes multas:

1.- Multas administrativas de 10.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía en caso de incumplimientos de las obligaciones:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

[27] Artículo 58 RGPD

[28] *Vid.* Grupo de Trabajo del Artículo 29 (2017), Directrices sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679, WP 253, 3 de octubre de 2017.

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.

2.- Multas administrativas de 20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía en los siguientes supuestos de incumplimientos:

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;

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.

Las sanciones mencionadas no son las únicas sanciones que se pueden imponer. También se permite que la sanción económica sea sustituida por otra o que la misma pueda ir aparejada con otras, en los supuestos que recoge el artículo 58 RGPD.

Si las infracciones fueran cometidas por instituciones u organismos de la UE, las sanciones sólo pueden ser de tipo disciplinario[29].

La LOPDGDD describe las conductas típicas en el Título IX y se clasifican las sanciones en muy graves, graves y leves teniendo en cuenta la diferenciación que el RGPD señala al fijar la cuantía de las sanciones. Se establecen también

[29] Así lo establece el art. 49 del Reglamento (UE) 2018/1725 de protección de datos de las instituciones de la UE.

los plazos de prescripción de acuerdo con la descripción de las conductas y se ejemplifican los actos sancionables que se entienden incluidos dentro de los tipos generales establecidos en la norma europea.