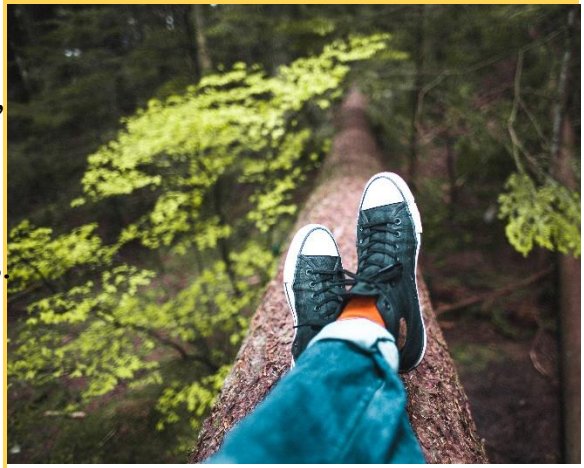
# Técnicos Auxiliares de Informática de la Administración del Estado 2019

TELEOPOSICIONES
**Avda. Maisonnave 28, bis 4ª Planta, Alicante**
temarios@teleoposiciones.es

Tema 9. La protección de datos personales. Régimen jurídico. El Reglamento (UE)2016/679, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Principios y derechos. Obligaciones. La Agencia de Protección de Datos: competencias y funciones.



El vigente Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, junto con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, configurarán desde el 25 de mayo de 2018 el nuevo marco europeo de protección de datos.

El nuevo Reglamento nace con un triple objeto:

- establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

- proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

- pretende que la libre circulación de los datos personales en la Unión no pueda ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

En relación con su ámbito de aplicación, se establecen dos distinciones:

Ámbito de aplicación material

El Reglamento se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos

personales contenidos o destinados a ser incluidos en un fichero. Por el contrario, no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Ámbito territorial:

Como matiza el art. 3 del Reglamento se aplica “al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.” Adquiriendo especial relevancia el punto 3 del citado artículo al matizar la aplicación: “al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.” Es decir, el Reglamento UE 2016/679, de 27 de abril de 2016 será aplicable al tratamiento de datos fuera de la Unión.

Principios rectores

La nueva norma se basa en los siguientes principios desarrollados en su capítulo II

Principios relativos al tratamiento. El responsable del tratamiento de los datos será responsable del cumplimiento y capaz de demostrarlo («responsabilidad proactiva»).

Licitud del tratamiento. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones especificadas en el apdo. 1, del art. 6.

Condiciones para el consentimiento. Cuando el tratamiento se base en el consentimiento se regulan las condiciones y características del mismo. En este apartado aparecen las «Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información»

Tratamiento de categorías especiales de datos personales. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. Esto no será de aplicación cuando concurra una de las circunstancias del apartado 2, art. 9.

Tratamiento de datos personales relativos a condenas e infracciones penales. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Tratamiento que no requiere identificación. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la

identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el Reglamento.

Fin de los derechos ARCO y llegada de transparencia, información, acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad de datos y oposición.

Los conocidos como derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) son el conjunto de derechos por los que actualmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, garantiza a las personas el control sobre sus datos personales. No obstante, con la llegada en 2018 del nuevo Reglamento Europeo, nacerán nuevos derechos superpuestos a los existentes en la LOPD:

Derecho de acceso del interesado (Art. 15)

Derecho de rectificación (Art. 16)

Derecho de supresión («el derecho al olvido») (Art. 17)

Derecho a la limitación del tratamiento (Art. 15)

Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento (Art. 19)

Derecho a la portabilidad de los datos (Art. 20)

Derecho de oposición (Art. 21)

Derecho a presentar una reclamación ante una autoridad de control (Art. 77)

Derecho a la tutela judicial efectiva contra una autoridad de control (Art. 78)

Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento (Art. 79)

Representación de los interesados (Art. 80)

Suspensión de los procedimientos (Art. 81)

Derecho a indemnización y responsabilidad (Art. 82)

¿Cuáles serán las novedades que incorporará el Reglamento?

La extensa regulación del Reglamento presentará novedades en aspectos como:

- Los ya citados principios aplicables al tratamiento de datos y Condiciones para el consentimiento.

- La regulación del denominado «derecho al olvido» o derecho de supresión de los datos personales. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias citada en el Art. 17.

- Derecho a la portabilidad de los datos. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se den las circunstancias citadas en el Art. 20.

- Responsabilidad del responsable del tratamiento. 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 el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

- Registro de las actividades de tratamiento. Cada responsable o encargado del tratamiento de datos (o su representante) realizarán un registro que deberá contener toda la información indicada en el art. 30

- Notificación de una violación de la seguridad de los datos personales a la autoridad de control. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

- Evaluación de impacto relativa a la protección de datos. El responsable del tratamiento de los datos realizará (en particular si utiliza nuevas tecnologías), antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

- Consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la

protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

- Regulación de las transferencias internacionales de datos. Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado (arts. 45-47).

- Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas (arts. 60 a 67).

Una nueva figura: el Delegado de protección de datos

Los arts. 37-39, crean una nueva figura, el Delegado de protección de datos, de esta forma a partir de 2018, El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

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.

Este delegado tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

BASE JURÍDICA

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que

respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ante la futura aplicación del Reglamento general de protección de datos de la UE para 2018, el Grupo de Autoridades europeas de protección de datos (GT 29), ha publicado directrices y respuestas a posibles dudas en relación con la portabilidad de datos, la figura de delegado de protección de datos y criterios de identificación de la autoridad de control.

Junto con el desarrollo de lo establecido por el GT enumeramos algunas cuestiones de necesario conocimiento en relación a la protección de datos.

I.- ¿Qué es el Grupo de Trabajo del Artículo 29?

II.- Reglamento general de protección de datos de la UE. Análisis y datos sobre su aplicación

III.- ¿Qué pasa con la Ley y el Reglamento de protección de datos nacional?

IV.- ¿Estoy preparado para la llegada del nuevo Reglamento General de Protección de Datos Personales Europeo? Principales novedades

V.- Portabilidad de datos, delegados de protección de datos y criterios de identificación de la «autoridad líder»

Derecho a la portabilidad de datos

Delegados de protección de datos

Autoridad de control principal

VI.- Nuevo régimen sancionador

I.- ¿Qué es el Grupo de Trabajo del Artículo 29?

El Grupo de Trabajo del Artículo 29 (GT 29), es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea creado por la Directiva 95/46/CE. A nivel estatal, la Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997.

Entre sus funciones se encuentran las de estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea.

Pueden consultar las directrices para la aplicación del Reglamento Europeo de Protección de Datos en GRUPO DE TRABAJO DEL ART.29

II.- Reglamento general de protección de datos de la UE. Análisis y datos sobre su aplicación

Como se estudia en nuestro “Análisis del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)”, el Reglamento UE 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (vigente desde el 24/05/2016), será aplicable a partir del 25 de mayo de 2018 afectando al conjunto de derechos a través de los cuales la actual Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, garantiza a las personas el poder de control sobre sus datos personales.

Reglamento (UE) 2016/679 de 27 de Abr DOUE (Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y derogación de la Directiva 95/46/CE (Reglamento general de protección de datos))

La norma se ha publicado en el DOUE el 4 de mayo de 2016. Es aplicable desde el 25 de mayo de 2016; pero su efectividad se producirá el 25 de mayo de 2018 [fecha en la que será de obligado cumplimiento en todos los Estados Miembros]. Su entrada en vigor supondrá la derogación de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El reglamento no afectará sólo a los europeos, su ámbito de aplicación integra a los responsables que no están en la Unión Europea, pero que ofrecen productos o servicios dentro de ella tratando datos de ciudadanos europeos.

III.- ¿Qué pasa con la Ley y el Reglamento de protección de datos nacional?

Pese a que en España existe la LOPD y su Reglamento de desarrollo, el reglamento europeo complementará, y en caso de contradicción sustituirá, la normativa nacional.

IV.- ¿Estoy preparado para la llegada del nuevo Reglamento General de Protección de Datos Personales Europeo? Principales novedades

En función del impacto que tendrá en las empresas la entrada en vigor del nuevo Reglamento Europeo, el test a realizar para verificar si estamos preparados se supedita a conocer las principales novedades y nuevas obligaciones:

A) Ampliaciones de las obligaciones respecto al deber de información a los usuarios y clientes: (arts. 13-15)

B) Resultará obligatorio el consentimiento explícito [bajo declaración o acción afirmativa] del usuario (arts. 7-11, 22)

C) Aparecen nuevas figuras: Delegados de protección de datos y «autoridad líder» y se regulan otras ya existentes como la portabilidad de datos.

Como analizamos más abajo, tener un "DPO" (Data Protection Officer) -en la empresa o a nivel externo- será imprescindible para organismos públicos y empresas que traten datos personales a gran escala.

D) Se exigirán evaluaciones de impacto antes de poder iniciar el tratamiento de los datos personales sensibles (arts. 35-36).

E) Derecho de supresión («el derecho al olvido»). El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias establecidas en el art. 17

F) Cuando los responsables de los datos observen alguna violación de la seguridad de los datos personales de un interesado deberán comunicarlo a la Autoridad correspondiente y al propio interesado lo antes posible. . Este punto, sin duda, traerá cola, el Reglamento manifiesta la necesidad de autodenuncia en caso de haber cometido un error en el tratamiento de datos (arts. 32-34):

"Artículo 33. Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

V.- Portabilidad de datos, delegados de protección de datos y criterios de identificación de la «autoridad líder»

Las citadas directrices publicadas por el GT 29 aclaran, en relación con la llegada del nuevo Reglamento general de protección de datos de la UE, tres aspectos regulados en la nueva norma:

Derecho a la portabilidad de datos

Partiendo de la regulación del artículo 20 -Derecho a la portabilidad de los datos- del RGPD, señalando que “el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a

transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado"

El GT 29 explica que este derecho se desglosa en las siguientes posibilidades para el afectado:

- recibir los datos personales relativos a su persona que está tratando el responsable y a almacenarlos en un dispositivo propio, sin comunicarlos a otro responsable del tratamiento. En este sentido, el GT 29 pone como ejemplo de aplicación práctica de este derecho el supuesto de un usuario que quiere obtener una lista de contactos de su webmail para preparar una lista de bodas, o el de un usuario de un servicio de música en streaming que quiere acceder a información sobre las canciones que más veces ha escuchado para comprarlas.

- solicitar al responsable del tratamiento que comunique sus datos a otro responsable. De esta forma, se permitirá la transmisión y reutilización de datos entre proveedores de servicios independientes con los que un mismo usuario mantiene una relación.

En esta guía se aclara igualmente que el derecho a la portabilidad no implica que los datos sean eliminados por el responsable del tratamiento ante quien se ejerce y que, en todo caso, éste deberá garantizar la seguridad de los datos personal en el proceso de transmisión.

Delegados de protección de datos

El art. 37 del RGPD -Designación del delegado de protección de datos- obliga al responsable y el encargado del tratamiento a designar un delegado de protección de datos siempre que:

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.

En base a la posible duda que generan ciertas expresiones en la regulación de la figura del DPO (abreviatura de las siglas en ingles de Data Protection Officer), se aclaran los conceptos “observación habitual y sistemática” y “tratamientos a gran escala”:

- Se considera tratamientos a gran escala por ejemplo:

Tratamientos de datos relacionados con los pacientes de un hospital.

Tratamiento de los datos de viaje de los usuarios del sistema de transporte público de una ciudad.

Tratamiento de datos de geolocalización en tiempo real de clientes para fines estadísticos.

Tratamiento de datos de clientes por una compañía de seguros o un banco.

Tratamiento de datos para la realización de actividades de publicidad comportamental online.

etc

Igualmente, son ejemplos de “observación habitual y sistemática”:

La gestión de una red de telecomunicaciones o la prestación de estos servicios

Actividades con la finalidad de realizar análisis de riesgos para prevención de blanqueo de capitales, prevención de fraude, análisis de riesgo crediticio, etc.

Tratamientos derivados de localización de usuarios a través de apps.

Programas de fidelización.

Tratamientos relacionados con publicidad conductual.

Tratamientos de datos de salud a través de dispositivos portátiles.

Tratamientos de datos datos derivados del uso de dispositivos conectados

etc.

Sobre esta figura la guía también propone ejemplos de incompatibilidades de ciertos cargos con la figura de DPO, su responsabilidad y la falta de certificación o titulación específica para ejercer las funciones (aunque quien ocupe este cargo deberá acreditar conocimientos específicos en la normativa nacional y europea de protección de datos).

Autoridad de control principal

Con base a la Sección 2 del Reglamento -Competencia, funciones y poderes- La guía propone ejemplos de tratamientos transfronterizos, y aclara los criterios para determinar qué autoridad debe ocupar el puesto de autoridad de control principal en diferentes supuestos.

VI.- Nuevo régimen sancionador

El art. 83, del Reglamento, relativo a las condiciones generales para la imposición de multas administrativas, establece un régimen sancionador mucho

más severo que el actual, sobre todo para aquellas empresas que tenga mayor facturación, citándose multas administrativas de 10 millones de euros, 20 millones de euros o de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

Del mismo modo, el art. 82, trata el derecho a indemnización y responsabilidad instaurando que "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos"