EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Módulo 4.

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

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

Contenido

4.1.- LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS.

4.1.1. ANTECEDENTES.

Tanto la LOPD como su Reglamento de desarrollo no regulan el Delegado de Protección de Datos, por lo que la introducción de este Delegado en el RGPD, supone una novedad en nuestro ordenamiento jurídico, si bien la Directiva 95/46 sí recogía la figura del Delegado de Protección de Datos, aunque con la denominación en su versión inglesa de la norma como "Data Protection Official", que en la traducción apareció como "encargado de la protección de datos".

Esta denominación como "encargado de la protección de datos" puede inducir a error, ya que podría confundirse con el "encargado del tratamiento", al que nos hemos referido en anteriores capítulos de este curso.

De esta forma, algunos países de la Unión Europea, al transponer la citada Directiva, contemplaron en sus respectivas normas el Delegado de Protección de Datos, como son los casos de Alemania y Eslovaquia.

Con anterioridad a la aprobación del RGPD, encontramos un mayor desarrollo del Delegado de Protección de Datos en el Reglamento 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000.

Este Reglamento se aplica en lo relativo al tratamiento de datos personales que se lleve a cabo por las instituciones y organismos comunitarios, así como la libre circulación de estos datos.

Según el considerando 32 de este Reglamento:

En cada institución u organismo comunitario, uno o varios responsables de la protección de datos velarán por que se aplique lo dispuesto en el presente Reglamento y asesorarán a los responsables del tratamiento en el ejercicio de sus obligaciones.

Por último, y en relación con los Delegados de Protección de Datos en el ámbito de las instituciones y organismos de la Unión Europea, el Supervisor Europeo de Protección de Datos (EDPS), publicó en noviembre de 2005 el documento "Position paper on the role of Data Protection Officers in ensuring efective compliance with Regulation (EC) 45/2001", donde analiza cuestiones como la independencia de actuación del Delegado así como sus funciones, clasificándolas de la siguiente forma: actividades destinadas a la concienciación; asesoramiento jurídico; cooperación; cumplimiento; administrativa-burocráticas; gestión de reclamaciones; y "enforcement".

4.1.2. OBLIGATORIEDAD, PERFIL Y APTITUDES.

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

- El tratamiento lo lleve a cabo una **autoridad u organismo público**, excepto los tribunales que actúen en ejercicio de su función judicial.
- Las **actividades principales** del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación **habitual y sistemática de interesados** a **gran escala**, o
- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de **categorías especiales de datos** personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

En este sentido, el Grupo del Artículo 29, a través del documento "Directrices sobre los delegados de la protección de datos", ha precisado lo siguiente sobre el supuesto de obligatoriedad en los Administraciones públicas:

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

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

En este sentido, y aprovechando esta posibilidad, el anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal que se está tramitando, recoge en su artículo 40 apartado 1 los siguientes supuestos en que se debe nombrar obligatoriamente un Delegado:

- Los colegios profesionales y sus consejos generales, regulados por la Ley 2/1974, de 13 febrero, de Colegios profesionales.
- Los centros docentes que ofrezcan enseñanzas reguladas por la Ley Orgánica 2/2006, de 3 de mayo, de Educación, y las Universidades públicas y privadas.

- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en la Ley 9/2014, de 9 de mayo, General de telecomunicaciones.
- Los prestadores de servicios de la sociedad de la información que recaben información de los usuarios de sus servicios, sea o no exigible el registro previo para la obtención de los mismos.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito regulados por Título II de la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial.
- Las entidades aseguradoras y reaseguradoras sometidas a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por el Título V del Texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.
- Los distribuidores y comercializadores de energía eléctrica, conforme a lo dispuesto en la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico, y los distribuidores y comercializadores de gas natural, conforme a la Ley 34/1998, de 7 de octubre, del Sector de hidrocarburos.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por el artículo 32 de la Ley 10/2010, de 28 de abril, de Prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales acerca de personas y empresas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a lo dispuesto en la Ley 3/2011, de 27 de mayo, de regulación del juego.
- Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Además, el apartado 2 de este artículo 40 del anteproyecto de nueva ley orgánica de protección de datos, recoge, sin perjuicio de estos supuestos de obligatoriedad, la posibilidad de que exista una designación voluntaria de un delegado de protección de datos.

Por otra parte, el RGPD determina que el Delegado de Protección de Datos en su artículo 37.5 y considerando 97 será una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos.

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

El Grupo del Artículo 29, que engloba a las Autoridades de Protección de Datos de la Unión Europea, entre las que se incluye obviamente la AEPD, a través del documento "Directrices sobre los delegados de la protección de datos", ha introducido al respecto las siguientes precisiones:

- **Conocimiento:**

  Aunque el Reglamento General de Protección de Datos no lo define, el nivel de conocimiento debe ser acorde con el tipo, cantidad y complejidad de datos que trate una organización.

- **Cualificación profesional:**

  Tampoco está precisado en el Reglamento General de Protección de Datos. No obstante, el Delegado de Protección de Datos debe tener conocimiento de las leyes tanto nacionales como europeas así como del mencionado Reglamento. En el ámbito privado, debe conocer el sector empresarial y en el ámbito público, un conocimiento sólido de las normas y procedimientos administrativos.

- **Capacidad:**

  Para desempeñar sus tareas debe tenerse en cuenta tanto sus cualidades personales y sus conocimientos como el puesto que ocupe en la organización. Entre las de carácter personas, se incluirían la integridad y un nivel elevado de ética profesional.

Si nos referimos al ámbito de las Administraciones Públicas, la provisión de los puestos de trabajo de Delegados de Protección de Datos requerirá la selección de empleados públicos que reúnan esos requisitos y, en especial, los conocimientos especializados en derecho y práctica la protección de datos que el Reglamento exige.

4.1.3. POSICIÓN EN LA ORGANIZACIÓN ADMINISTRATIVA.

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

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

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

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

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

Al mismo tiempo, no parece aconsejable que ese único Delegado actúe respecto de grandes unidades u órganos con entidad y tareas claramente diferenciadas, por mucho que orgánicamente puedan depender de un departamento ministerial, consejería o ayuntamiento (podrían ser ejemplos los casos de la Secretaría de Estado de Seguridad Social, responsable de la dirección y tutela de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, o el de la Dirección General de Tráfico).

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

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

En órganos, organismos o entes de gran tamaño en que exista un único Delegado lo habitual será que desempeñe sus funciones a tiempo completo. Es, incluso, posible

que el Delegado formalmente nombrado esté respaldado por una unidad específicamente dedicada a la protección de datos.

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

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

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

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

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

- La participación de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales;
- Recibir el apoyo del responsable o encargado, que deberán facilitarle los recursos necesarios para el desempeño de sus funciones ;
- No recibir ninguna instrucción en lo que respecta al desempeño de dichas funciones y no ser destituido ni sancionado por el responsable o el encargado por causas relacionadas con ese desempeño de funciones;
- Rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado. Esta característica debe interpretarse en el sentido de que el Delegado debe poder relacionarse con niveles jerárquicos que tengan la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones que realice.
- Invitar al Delegado a participar con regularidad en las reuniones de los cuadros directivos altos y medios.
- Presencia en la toma de decisiones con implicaciones para la protección de datos, de forma que toda la información relevante se le transmita de manera oportuna para que pueda prestar un asesoramiento adecuado.
- Su opinión debe gozar siempre de la consideración oportuna, documentando las razones para no seguir su consejo.
- Se le debe consultar tan pronto se produzca una violación de datos u otro incidente.

Además, según el documento del Grupo del Artículo 29 "Directrices sobre los Delegados de Protección de Datos", debe tenerse en consideración los elementos referentes:

- **Recursos:** El artículo 38.2 del Reglamento determina que la organización debe apoyar al Delegado proporcionándole los recursos necesarios para realizar sus funciones así como el acceso a los datos personales y operaciones de tratamiento, así como para mantener su conocimiento experto. Por parte de la alta dirección, debe existir un apoyo activo a las funciones que realice el Delegado, como el tiempo suficiente para el ejercicio de las mismas; dotación de recursos económicos, infraestructura y personal; acceso a otros servicios (recursos humanos, departamento jurídico, tecnologías de la información) que puedan apoyar al Delegado; y equipo de personas a cargo del Delegado en función de la estructura de la organización.

- **Independencia:** El artículo 38.3 del Reglamento establece unas garantías básicas para que los Delegados actúen con independencia dentro de la organización en la que prestan sus servicios, incluyendo que *"no reciban ninguna instrucción relativa al ejercicio de sus tareas"*. Además, es importante señalar que los obligados al cumplimiento del RGPD son el responsable o el encargado del tratamiento, de forma que si adoptan decisiones contrarias a la norma y al asesoramiento prestado por el Delegado, debe darse a éste la posibilidad de expresar con claridad su opinión disconforme respecto a dichas decisiones.

- **Destitución:** El anteriormente citado artículo 38.3 también se refiere a que los Delegados de Protección de Datos "no deben ser destituidos ni penalizados por el responsable o el encargado por llevar a cabo sus funciones", lo que supone un refuerzo de su autonomía e independencia. Sí podría ser despedido o sancionado de conformidad con la legislación contractual, laboral o penal aplicable de cada país, por causas distintas al desempeño de sus funciones (por ejemplo, por robo o acoso sexual). Téngase en cuenta en el ámbito de las Administraciones públicas el régimen de infracciones y sanciones aplicables a su personal.

- **Conflicto de interés:** Si bien el Delegado de Protección de Datos puede realizar otras funciones en la organización, éstas no pueden suponer un conflicto de intereses. Por ello, y atendiendo a la estructura, actividades y tamaño de cada organización, se recomienda que responsables o encargados del tratamiento: determinen los puestos que serían incompatibles con las funciones del Delegado; elaboren normas internas para evitar estos conflictos; declarar que el Delegado no tiene conflicto de intereses en relación con sus funciones; inclusión de salvaguardas en normas internas y garantizar que el

anuncio de la vacante para Delegado o el contrato de servicios sea lo suficientemente preciso y detallado para evitar los citados conflictos.

4.1.4. FUNCIONES.

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

- **Respecto al cumplimiento:**

  - Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
  - Identificación de las bases jurídicas de los tratamientos.
  - Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
  - Existencia de normativa sectorial que pueda determinar condiciones de tratamientos específicos distintas de las establecidas por la normativa general de protección de datos.
  - Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
  - Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
  - Diseño e implantación de políticas de protección de datos.
  - Auditoría de protección de datos.
  - Establecimiento y gestión de los registros de actividades de tratamiento.

- **Respecto a la relación con los interesados:**

  - Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
  - Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
  - Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

- **Respecto a la Seguridad:**

  - Análisis de riesgo de los tratamientos realizados.
  - Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

- **Respecto a la Prevención:**

  - Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
  - Realización de evaluaciones de impacto sobre la protección de datos.
  - Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

- **Respecto a la Cooperación:**

  - Relaciones con las autoridades de supervisión.

- **Respecto a la Formación:**

  - Implantación de programas de formación y sensibilización del personal en materia de protección de datos

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

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

- **Relación con las Autoridades de Control de Protección de Datos (artículo 57.3):** Las relaciones entre el Delegado de Protección de Datos y su respectiva Autoridad de Control serán gratuitas, sin coste económico que tenga que sufragar la entidad que haya designado al Delegado.

4.2.- CÓDIGOS DE CONDUCTA.

Los **códigos tipo**, de acuerdo con la denominación utilizada por la Directiva 95/46 y la LOPD y su reglamento de desarrollo o **códigos conducta**, de acuerdo con el término utilizado en el RGPD, constituyen una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse a sí mismas. En el ámbito de la protección de datos esa capacidad está orientada a la adopción de reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por aquellas instituciones, entidades o empresas, adheridas al código tipo o que lo promuevan, a facilitar el ejercicio de los derechos de los afectados, favorecer el cumplimiento de la normativa de protección de datos así como instrumento que puede ser utilizado por los responsables y encargados para demostrar el cumplimiento de dicha normativa.

Con la adopción de los códigos tipo los responsables y los encargados de los tratamientos pueden adecuar a las características del sector en que operen las previsiones normativas de protección de datos y ampliarlas, ofreciendo transparencia en cuanto a su actuación. Son instrumentos que aportan un valor añadido a la regulación.

Característica fundamental de los códigos tipo, derivadas de su naturaleza de autorregulación, es el carácter voluntario de la adhesión, siendo vinculantes para todas las instituciones o entidades una vez adheridas a los mismos.

En el marco de la autorregulación y del principio de responsabilidad proactiva que el RGPD pretende promover, los códigos de conducta, junto con las certificaciones, destacan como una herramienta útil para demostrar que los responsables y los encargados cumplen con los requisitos establecidos en el Reglamento europeo.

Los códigos de conducta, a diferencia de las certificaciones, ya estaban previstos de una forma genérica en la Directiva 95/46/CE y, en el caso de España, se adaptó al derecho nacional tanto en la LORTAD de 1992 como en la todavía vigente LOPD.

El objetivo principal del RGPD al dar una mayor relevancia a los códigos de conducta es la de que sirvan como herramientas para que los responsables y encargados puedan demostrar su cumplimiento, teniendo en cuenta las características y necesidades específicas de los distintos sectores y de las PYMEs y micropymes. Para ello, señala a los Estados miembros, las autoridades de protección de datos, el Comité europeo de protección de datos, así como a la Comisión, como impulsores para la elaboración de códigos de conducta o para la adaptación de los ya existentes por parte de los responsables y encargados, así como a las asociaciones y otros organismos representativos de categorías de responsables y encargados.

El RGPD señala los aspectos que, ente otros, estos códigos deberían incluir, lo que podría entenderse como un conjunto de requisitos mínimos a ser abordados con el fin

de contribuir a la correcta aplicación del Reglamento europeo. Para ello, según señala el artículo 40 del RGPD, las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar aquellos códigos con objeto de especificar la aplicación del RGPD, en lo que respecta a:

- el tratamiento leal y transparente;
- los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
- la recogida de datos personales;
- la seudoanonimización de datos personales;
- la información proporcionada al público y a los interesados;
- el ejercicio de los derechos de los interesados;
- la información proporcionada a los niños y la protección de éstos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
- las medidas y procedimientos para garantizar la seguridad del tratamiento así como la protección de datos desde el diseño y por defecto;
- la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
- la transferencia de datos personales a terceros países y organizaciones internacionales, o
- los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativos al tratamiento, sin perjuicio de los derechos de los interesados.

Destaca este último aspecto, que permitirá resolver los conflictos que pudieran plantearse y obtener satisfacción de manera ágil.

El RGPD prevé la posibilidad de aprobar códigos de conducta cuando guarde relación con actividades de tratamiento en varios Estados miembros o incluya compromisos vinculantes y exigibles para realizar transferencias internacionales de datos a través del mecanismo de coherencia que cuenta como antecedente el mecanismo coordinado y de reconocimiento mutuo impulsado por el Grupo del Artículo 29 (*este Grupo está formado por las Autoridades de Protección de Datos de la Unión Europea*) para la adopción de las BCR.

Mucho más impreciso parece, por el momento, el alcance del mecanismo previsto para la supervisión de códigos de conducta por parte de un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente, por lo que habrá que esperar a ver la aplicación práctica prevista en el artículo 41 del RGPD.

Como resumen, los códigos de conducta, que adquieren una mayor relevancia, resultan un instrumento que no sólo permite adecuar la aplicación del RGPD a las características de cada sector, sino que sirven para demostrar su cumplimiento y, en el caso de España, tanto la AEPD como los potenciales promotores de los códigos disponen de un buen punto de partida en la experiencia desarrollada durante la vigencia de la LOPD y, en especial, de su reglamento de desarrollo.

Con respecto a los procedimientos de elaboración y adopción habría que distinguir dos supuestos:

- **Códigos de ámbito exclusivamente nacional:**

  Los códigos de conducta serán aprobados por la AEPD o, en su caso, por la autoridad autonómica de protección de datos competente previa evaluación de su conformidad con el RGPD.

  La AEPD y las autoridades autonómicas de protección de datos mantendrán un registro de los códigos de conducta aprobados por las mismas y los aprobados conforme al mecanismo de coherencia establecido en el artículo 63 del RGPD.

- **Códigos que afectan a tratamientos en varios estados de la UE:**

  La AEPD y, en su caso, las autoridades autonómicas de protección de datos, enviarán el código de conducta, antes de su aprobación, al Consejo Europeo de Protección de datos para la emisión del dictamen sobre su adecuación al RGPD y/o dictamen sobre las garantías ofrecidas para las transferencias internacionales de datos, procediéndose a la suspensión del procedimiento hasta la emisión del informe.

  Si el dictamen fuera favorable, el Consejo Europeo de Protección de Datos lo presentará a la Comisión, que decidirá sobre que el código tenga validez dentro de la UE y, en ese caso, le dará publicidad.

  El Consejo Europeo de Protección de Datos llevará un registro de los códigos de conducta que afecten a tratamientos en varios estados de la UE y los pondrá a disposición pública.

El Anteproyecto de LOPD amplía el ámbito de los promotores al extenderlo también a las empresas y grupos de empresas, así como a las entidades del Sector Público.

4.3. ESQUEMAS DE CERTIFICACIÓN.

4.3.1. LÍNEAS GENERALES DE LA CERTIFICACIÓN.

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

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

En consecuencia, procede diferenciar lo siguiente:

- **Certificación**: proceso metodológico de evaluación mediante el cual una tercera parte garantiza la conformidad de una persona, un producto, servicio o sistema de información con unos criterios preestablecidos.

- **Esquema de Certificación:** aquel que establece las reglas, los procedimientos y las gestiones que deben realizar aquellas personas, organizaciones públicas o privadas que desean certificarse.

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

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

- Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos y aprobar los criterios de certificación.

- Llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas.

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

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

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

- El organismo que elabora las normas técnicas que determinan los requisitos específicos de la certificación (esquema de certificación).

- La entidad u organismo de certificación que es la que emite el documento oficial que demuestra el cumplimiento de las normas técnicas.

- La entidad o persona certificada.

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

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

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

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

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

- Que hayan demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto de la certificación.

- Si se han comprometido a expedir la certificación sobre la base de los criterios aprobados por la autoridad de control.

- Si han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificación, sellos y marcas de protección de datos.

- Han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público.

- Han demostrado, a satisfacción de la autoridad de control, que sus funciones y cometidos no dan lugar a conflicto de intereses.

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

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

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

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

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

4.2. ESPECIAL CONSIDERACIÓN A LA CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS.

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

No obstante, la norma también recoge otra posible certificación, que es la del delegado de protección de datos.

Aunque la AEPD tiene entre sus objetivos desarrollar el esquema de certificación en materia de cumplimiento, para dar una seguridad jurídica a la profesión de delegado de protección de datos y a aquellas entidades que por obligación tienen que nombrar uno o necesitan el asesoramiento de un profesional cualificado, ha optado por definir el esquema de certificación que regule las funciones del delegado de protección de datos.

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

Por tanto, la AEPD se ha convertido en la primera autoridad europea que realiza un esquema de certificación de Delegados de Protección de Datos. Para su elaboración se ha contado con la participación de un Comité Técnico de Expertos de 23 miembros, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas.

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

- El organismo propietario del esquema de certificación es la Agencia Española de Protección de Datos apoyada y asesorada por un Comité Técnico representado por aquellas asociaciones sectoriales cuyos asociados están obligados a nombrar un delegado de protección de datos, así como entidades que ya cuentan con un certificado de profesionales de la privacidad además de representantes de las universidades.

- ENAC, encargada de que las entidades de certificación cumplan los requisitos necesarios para acreditarse como tales.

- Las entidades de certificación son las que emiten el documento oficial que certifica que el Delegado de Protección de Datos cumple con los requisitos exigidos por el Esquema de Certificación, dispone de los conocimientos necesarios y está en disposición de ejercer sus funciones como tal profesional.

La AEPD ha decidido que la acreditación de las entidades de certificación sea realizada por ENAC, por lo que cualquier entidad que desee ser certificadora del Esquema deben solicitar a ENAC la acreditación como tal para lo cual deben pasar un proceso regulado por la normativa correspondiente y una vez superado el mismo, ENAC emitirá la correspondiente acreditación que será supervisada en todo momento por la AEPD.

La Agencia, cuando valoro cómo abordar la elaboración de este esquema de certificación consideró esta división la mejor opción ya que representa un factor de calidad para el proceso de certificación al tratarse de tres entidades diferentes con funciones independientes.

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

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

Por último, indicar que en la página web de la AEPD se pueden consultar los siguientes documentos al respecto:

- Esquema de certificación.
- Anexo II. A. Norma de uso de la marca.
- Anexo I.B Condiciones de justificación de los prerrequisitos.
- Anexo II.B Modelo de contrato de uso de marca.
- Anexo IV Código ético del delegado de protección de datos.
- Anexo V Programa del esquema.
- Anexo VI Procedimiento de selección y designación de evaluadores.
- Anexo VII Certificación de conformidad con el esquema.

4.4. TRANSFERENCIAS INTERNACIONALES DE DATOS.

4.4.1. MARCO GENERAL DE LAS TRANSFERENCIAS

El RGPD señala en su Considerando 6 que "*La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales*".

Según el Considerando 101 del citado RGPD, "*Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena*

conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales".

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

Sin embargo, dado que el RGPD no incluye una definición de transferencia internacional de datos quizás resulte adecuado, a efectos de claridad didáctica y con carácter general, se puede tener de referencia la definición todavía vigente del artículo 5.1.s) del RLOPD:

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

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

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

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

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

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

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

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

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

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

La normativa aplicable en España hasta mayo de 2018 obliga a los exportadores de datos a solicitar una autorización previa para poder transferir datos a importadores establecidos en países que no cuentan con un nivel adecuado de protección, siempre

que aporten las garantías suficientes, y a notificar las transferencias cuando se dirigen a países que sí disponen de dicho nivel adecuado o, en otro caso, se realizan al amparo de alguna de las excepciones previstas en la LOPD.

Sin embargo, en el marco del RGPD, con carácter general, las transferencias se pueden llevar a cabo sin necesidad de autorización previa, salvo que las garantías se aporten a través de un contrato entre el responsable o el encargado del tratamiento, encargado o destinatario de los datos personales en el tercer país u organización internacional, o de un acuerdo administrativo entre autoridades públicas, supuestos en los que será preciso que exista la autorización de la autoridad de control, tal y como señala el artículo 46.3 del RGPD.

4.4.2. TRANSFERENCIAS BASADAS EN UNA DECISIÓN ADECUADA.

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

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

- Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda.
- Canadá (sólo cuando a la entidad destinataria le sea de aplicación la "Personal Information and Electronic Documents Act").
- Estados Unidos (sólo cuando la entidad destinataria de los datos este certificada en el esquema del Escudo de Privacidad).

4.4.3. TRANSFERENCIAS MEDIANTE GARANTÍAS ADECUADAS.

De conformidad con el Considerando 108 del RGPD "*En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por*

defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente".

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

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

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

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

4.4.4. NORMAS CORPORATIVAS VINCULANTES.

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

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

Para su aprobación por la autoridad de control competente, el RGPD establece una serie de requisitos que se han plasmado en diversos documentos elaborados por el denominado Grupo del Artículo 29 de la Directiva 95/46[1]. En este grupo se reúnen todas las autoridades de control de la UE y será sustituido por el Comité europeo de protección de datos a partir del 25 de mayo de 2018.

Estos requisitos se enumeran en el artículo 47 del RGPD:

- sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

- confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales; y

- cumplan e incluyan, como mínimo los siguientes requisitos y elementos:

  a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

  b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

  c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

  d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

[1] WP 74, WP 107, WP 108, WP 133, WP 153, WP 155, WP 195 y WP 204. Pueden ser consultados en la siguiente dirección:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14 relativos a la información que debe facilitarse a los interesados;

h) las funciones de todo delegado de protección de datos designado, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la

unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

4.4.5 EXCEPCIONES PARA SITUACIONES ESPECÍFICAS.

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

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

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

transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados".

Dado que se consideran excepciones al régimen general, el RGPD, como ya lo hizo el Grupo del artículo 29 en su documento WP 114[2], quiere clarificar el régimen restrictivo del uso de dichas excepciones, por lo que conforme al Considerando 113: "*Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado*".

Así, el anteproyecto de LOPD señala como supuesto que deberá ser previamente comunicado a la autoridad de protección de datos competente cuando la transferencia internacional se pretenda llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos del responsable, así como a los afectados por la transferencia.

4.5 CASO PRÁCTICO

Un hospital público, de pequeño tamaño, recibe la visita de un profesional de la privacidad que oferta sus servicios como delegado de protección de datos para:

- Adaptar los ficheros que actualmente posee el hospital al contenido del RGPD;
- Que le nombren como delegado de protección de datos.

Los ficheros actuales del hospital son los siguientes:

- Pacientes;
- Lista de espera;

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

- Urgencias;
- Quirófanos;
- Personal;
- Investigación clínica.

Estos ficheros se ajustan a lo dispuesto en la LOPD y su Reglamento de desarrollo, tanto en lo referente a principios, obligaciones así como lo relativo a las medidas de seguridad. Estas medidas son de nivel alto en la mayoría de esos ficheros, al tratar datos de salud.

El hospital cuenta con un responsable de seguridad, que iba a ser designado por la Dirección de este centro de salud como Delegado de Protección de Datos.

Los servicios que le oferta el delegado de protección de datos son los siguientes:

- Asesorar al responsable del hospital sobre el contenido del RGPD.
- Actualizar los ficheros citados al nuevo registro de ficheros que está preparando la AEPD, para que los citados ficheros se adecúen al RGPD.
- Asignar responsabilidades al personal del hospital.
- Formar al personal.
- Implementar el nuevo nivel de seguridad, denominado "muy alto", que regula el RGPD respecto a los datos de salud.
- Tramitar las denuncias ante la Agencia Española de Protección.
- Gestionar las tutelas de derechos.
- Elaborar las evaluaciones de impacto.
- Diseñar e implantar las políticas de protección de datos.

CUESTIONES PLANTEADAS.

1.- ¿Debe este hospital nombrar un delegado de protección de datos?

2.- Si nombrase un delegado de protección de datos ¿Podría ser externo o debe ser personal del hospital?

3.- ¿Podría el hospital nombrar como delegado de protección de datos al responsable de seguridad?

4.- ¿Debería elegir ese hospital a ese profesional como delegado de protección de datos atendiendo a los servicios que presta?

SOLUCIÓN.

1.- El hospital debería designar una delegado de protección de datos debido a que se trata de un organismo público, según lo que dispone el artículo 37.1.a) del RGPD.

Además, también debería designarlo puesto que su actividad principal consiste en un tratamiento a gran escala de categoría especiales de datos personales, entre los que se encuentran los datos de salud.

El Grupo del Artículo 29, a través del documento "Directrices sobre los delegados de protección de datos", que puede consultarse en la documentación adicional de este módulo, ha clarificado que se entiende por "actividad principal" y "gran escala", incluyendo a los hospitales entre los que deben designar un delegado de protección de datos obligatorio.

2.- El RGPD no se pronuncia sobre este aspecto, por lo que corresponde al responsable determinar si se designa personal interno, o se recurre a contratar a alguien externo.

En el caso de que haya una contratación externa, se puede realizar con una empresa. La nueva Ley Orgánica de Protección de Datos que se está tramitando, recoge en su artículo 36 que el Delegado de Protección de Datos puede ser una persona física o jurídica.

En el documento publicado por esta AEPD "El delegado de protección de datos en las Administraciones públicas", que puede consultarse en la documentación adicional de este módulo, se analiza este supuesto de contratación interna o externa.

Concretamente se señala lo siguiente:

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

3.- El RGPD establece en su artículo 38.6 que "El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a un conflicto de intereses".

Por tanto, no puede ser nombrado el responsable de seguridad, ya que de realizar dicho nombramiento podría existir un conflicto de intereses entre las funciones como responsable de seguridad y las relativas a delegado de protección de datos.

En el documento publicado por esta AEPD "El delegado de protección de datos en las Administraciones públicas", que puede consultarse en la documentación adicional de este módulo, se especifica a este respecto:

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

4.- La oferta que ha realizado el DPD externo no es clara y parece desprenderse que se trata de un profesional de la privacidad que, aunque oferta sus servicios con delegado, desconoce cuáles son las funciones de un DPD según se describe en el RGPD.

Según el RGPD, artículo 39, las funciones serían como mínimo

- informar y asesorar al responsable y a los empleados que se ocupen del tratamiento de las obligaciones que les incumplen en virtud del RGPD y el resto de la normativa de protección de datos aplicable;
- supervisar el cumplimiento del RGPD incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorias correspondientes.
- asesorar sobre las evaluaciones de impacto y supervisar su aplicación, cooperar con la autoridad de control así como actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento incluida la consulta previa.

En la oferta propuesta, los servicios que pretende ejecutar son los de un profesional de la privacidad, pero carece de los conocimientos suficientes del RGPD.

Ejemplos al respecto podemos encontrar los siguientes:

- El RGPD no establece ningún nuevo registro de ficheros, es más, establece la no obligación de inscripción de ficheros que sí regula los todavía vigentes LOPD así como su Reglamento de desarrollo. Lo que regula el RGPD, que se ha explicado en el Módulo 3 de este curso, es el Registro de Actividades de Tratamiento.

- El RGPD, a diferencia del Reglamento de desarrollo de la LOPD, no configura las medidas de seguridad en función del tipo de datos que se trate asignando niveles de seguridad al respecto. Esta cuestión se ha explicado también en el Módulo 3 de este curso.