Primicia: Así deben ser los Delegados de Protección de Datos, el trabajo ciber de moda en 2018, según la Agencia Española de Protección de Datos.

POR JOSÉ M. VERA
MÁS ARTÍCULOS DE ESTE AUTOR
Miércoles 12 de julio de 2017, 12:58h

http://www.onemagazine.es/asi-debe-ser-el-delegado-de-proteccion-de-datos-2018-normativa-europea-datos-rgpd-aepd

Los expertos de la Agencia Española de Protección de Datos responden en una amplia entrevista a cómo debe ser -y como no- el Delegado de Protección de Datos -DPD- que velará en las empresas porque se cumplan los requisitos, para protegerlos, del nuevo reglamento europeo. Desde el 25 de mayo entrarán en vigor sus multas de hasta 20 millones de euros. Aclara dudas...

El nuevo reglamento europeo de datos ya está en vigor. Sin embargo, cada país está haciendo la transposición de la normativa. España acaba de publicar el anteproyecto de Ley que está actualmente en 'consulta pública' para que ciudadanos y empresas propongan cambios. De cualquier forma, la Ley europea se aplica ya en todos los países. Eso sí, hasta el 25 de mayo de 2018 no estarán vigentes las sanciones de hasta 20 millones de euros por no cumplir sus exigencias para proteger los datos personales de los clientes.

La normativa impondrá nuevos derechos, como el de portabilidad de datos cuando dejas una empresa, y también un nuevo perfil profesional: el Delegado de Protección de Datos -DPD-, que dependerá del responsable de la empresa, será independiente y se encargará de garantizar que los datos se tratan y protegen conforme a la Ley. Sin embargo, este nuevo perfil profesional también está suscitando mucho debate en el mundo de la cibersegurida acerca de quién estará capacitado para ejercer como tal, si los responsables de Tecnología de la Información o de ciberseguridad pueden serlo y cómo se integra el DPD en el organigrama de la empresa, debatidos en foros como las jornadas que organiza la asociación de ejecutivos de ciberseguridad ISMS Forum.

Para aclarar dudas hemos preguntado a los expertos de la Agencia Española de Protección de Datos -que este 13 de julio presenta cómo deberán certificarse los nuevos DPD-. Estas han sido sus respuestas y las recomendaciones que deben tener en cuenta todas las empresas:

¿Que hay que saber sobre los Delegados de Protección de Datos?

1.-¿Qué cinco características tiene que cumplir este perfil en España?

El Reglamento Europeo de Protección de Datos -RGPD- establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

• Autoridades y organismos públicos

• Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala

• Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos o el tratamiento de datos sensibles.

Según el RGPD, la posición del DPD debe conllevar:

- 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 DPD debe poder relacionarse con niveles jerárquicos que tengan la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones que realice el DPD.

Todos estos elementos deben ser tomados en consideración en la identificación de la ubicación del DPD dentro de la organización y en la configuración del correspondiente puesto de trabajo y, en su caso, de la unidad dependiente del DPD. La designación del DPD y sus datos de contacto deben

hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.

2.-Si alguien quiere trabajar como DPD, ¿cómo se tiene que formar? ¿Desde qué trabajos, puestos o estudios se puede ser DPD?

El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. El RGPD establece que el DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar sus funciones.

Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

¿Qué dice la normativa sobre el DPD?

El Grupo de Autoridades Europeas de los Estados miembros (GT29) ha publicado unas Directrices sobre la designación de los DPD que especifican lo siguiente: El artículo 37(5) estipula que el DPD "se designará en función de su cualificación profesional y, en especial, su conocimiento experto de la legislación y las prácticas de protección de datos así como su capacidad de desempeñar las tareas a las que hace referencia el artículo 39". El considerando 97 establece que debe determinarse el nivel necesario de conocimiento experto de acuerdo con las operaciones de tratamiento de datos llevadas a cabo y la protección requerida para los datos personales que se están tratando.

• **Nivel de conocimiento** El nivel de conocimiento requerido no está definido estrictamente pero debe ser acorde con el carácter sensible, la complejidad y la cantidad de datos que procesa una organización. Por ejemplo, cuando una actividad de tratamiento de datos es especialmente compleja, o cuando implica una gran cantidad de datos sensibles, el DPD podrá requerir un nivel mayor de conocimiento y apoyo. Existe también una diferencia dependiendo de si la organización transfiere sistemáticamente datos personales fuera de la Unión Europea o si tales transferencias son ocasionales. Así pues, el DPD debe elegirse con cuidado, teniendo en cuenta debidamente los problemas de protección de datos que surjan dentro de la organización

• **Cualificación profesional** Aunque el artículo 37(5) no especifica la cualificación profesional que debe tenerse en cuenta al designar un DPD, un aspecto importante es que los DPD deben tener

conocimiento de las leyes y prácticas de protección de datos tanto nacionales como europeas y una comprensión profunda del RGPD. Resulta útil también que las autoridades supervisoras promuevan una formación adecuada y regular para los DPD. Es de utilidad el conocimiento que el responsable del tratamiento tenga del sector empresarial y la organización, incluyendo cuestiones normativas o reglamentarias.

El DPD debe tener suficiente comprensión de las operaciones de tratamiento llevadas a cabo y los sistemas de información, así como las necesidades de seguridad y protección de los datos del responsable del tratamiento. En el caso de una autoridad u organismo públicos, el DPD debe tener también un conocimiento sólido de las normas y procedimientos administrativos de la organización.

• **Capacidad de desempeño de sus tareas** La capacidad de desempeño de las tareas propias del DPD debe medirse tanto por sus cualidades personales y sus conocimientos como por el puesto dentro de la organización. Las cualidades personales deben incluir, por ejemplo, la integridad y un nivel elevado de ética profesional; la principal preocupación del DPD debe ser hacer posible el cumplimiento del RGPD. El DPD desempeña un papel clave a la hora de promover una cultura de protección de datos dentro de la organización y ayuda a implementar elementos esenciales del RGPD, como son los principios del tratamiento de datos, los derechos de los interesados, la protección de datos por diseño y por defecto, los registros de actividades de tratamiento, la seguridad del tratamiento y la notificación y comunicación de violaciones de datos.

3.-¿Quién no puede ser DPD de una empresa -por ejemplo, lo puede ser el CISO, el CIO, el CTO...-?

El RGPD prevé que el DPD podrá desarrollar su actividad a tiempo completo o a tiempo 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 DPD lo habitual será que desempeñe sus funciones a tiempo completo.

Es, incluso, posible que el DPD formalmente nombrado esté respaldado por una unidad específicamente dedicada a la protección de datos. En entidades de menor tamaño será posible que el DPD 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. 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.

En las Directrices publicadas por el GT29 se especifica lo siguiente: El artículo 38(6) permite a los DPD "desempeñar otras tareas y funciones". No obstante, exige que la organización garantice que

"tales tareas y funciones no deriven en un conflicto de interés". La ausencia de conflicto de interés está estrechamente ligada al requisito de actuar con independencia. Aunque se permite a los DPD tener otras funciones, solo se les puede confiar otras tareas y funciones siempre que estas no originen conflictos de interés.

Esto supone en especial que el DPD no puede detentar un cargo dentro de la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso. Por regla general, los cargos en conflicto pueden incluir los puestos de alta dirección -tales como director ejecutivo, director de operaciones, director económico financiero, director médico, jefe del departamento de marketing, director de recursos humanos o jefe del departamento de TI-, pero también otros puestos inferiores en la estructura organizativa si tales cargos o funciones llevan a la determinación de los fines y medios del tratamiento.

Dependiendo de las actividades, el tamaño y la estructura de la organización, puede ser recomendable para los responsables o encargados del tratamiento:

• Determinar qué puestos serían incompatibles con la función de DPD

• Redactar normas internas a estos efectos para evitar conflictos de interés

• Incluir una explicación más general sobre los conflictos de interés

• Declarar que su DPD no tiene ningún conflicto de interés en relación con su función como DPD, como medio de concienciar sobre este requisito

• Incluir salvaguardas en las normas internas de la organización y garantizar que el anuncio de vacante para el puesto de DPD o el contrato de servicios sea lo suficientemente preciso y detallado para evitar un conflicto de interés. En este contexto, debe tenerse en cuenta que los conflictos de interés pueden adoptar diversas formas en función de si el DPD se contrata interna o externamente.

4.-¿Cuáles son las exigencias del nuevo reglamento respecto al DPD y qué papel tiene que jugar la empresa con él -por ejemplo, cómo se constará que se le han dado medios si hay una brecha para que él no esgrima este aspecto para evadir la responsabilidad?

Los DPD no son personalmente responsables en caso de incumplimiento del RGPD. El RGPD declara taxativamente que son el responsable y el encargado del tratamiento quienes están obligados a garantizar y poder demostrar que el tratamiento se lleva a cabo con arreglo a sus disposiciones -artículo 24(1)-. La protección de datos es responsabilidad del responsable o el encargado del

tratamiento, quienes asimismo tienen un papel crucial a la hora de hacer posible el desempeño efectivo de las tareas del DPD. El nombramiento de un DPD es el primer paso, pero debe conferírsele suficiente autonomía y recursos para que lleve a cabo su cometido de forma efectiva.

Las **Directrices publicadas por el GT29** especifican lo siguiente: El artículo 38(3) establece unas garantías básicas para ayudar a asegurar que los DPD puedan llevar a cabo sus tareas con el suficiente grado de autonomía dentro de su organización. En especial, los responsables y encargados del tratamiento están obligados a garantizar que el DPD "no reciba ninguna instrucción relativa al ejercicio de sus tareas». El considerando 97 añade que los DPD, "sean o no un empleado del responsable del tratamiento, deben estar en condiciones de desempeñar sus tareas y funciones con total independencia" Esto significa que, en el desempeño de sus tareas según el artículo 39, los DPD no deben recibir instrucciones sobre el modo de ocuparse de un asunto, por ejemplo, sobre el resultado que debe alcanzarse, sobre el modo de investigar una queja o sobre si debe consultarse a la autoridad supervisora. Asimismo, no deben recibir instrucciones de adoptar una determinada postura sobre una cuestión relacionada con la legislación de protección de datos, por ejemplo, una interpretación concreta de la ley.

La autonomía de los DPD no significa, sin embargo, que tengan la potestad de tomar decisiones que vayan más allá de sus funciones definidas con arreglo al artículo 39. El responsable o el encargado del tratamiento sigue siendo el responsable del cumplimiento de la ley de protección de datos y debe poder demostrarlo. Si el responsable o el encargado toma decisiones que sean incompatibles con la RGPD y el consejo del DPD, deberá darse la posibilidad al DPD de expresar con claridad su opinión disconforme ante los responsables de dichas decisiones.

El artículo 38(2) de la RGPD estipula que la organización debe respaldar a su DPD "proporcionando los recursos necesarios para que lleve a cabo sus tareas y acceda a los datos personales y las operaciones de tratamiento, así como para mantener su conocimiento experto". Deben tenerse en cuenta, en especial, los siguientes aspectos:

• **Apoyo activo a la función del DPD** por parte de la alta dirección (como puede ser el consejo de administración). Tiempo suficiente para que los DPD cumplan con sus funciones. Esto es especialmente importante cuando se designa al DPD a tiempo parcial o cuando el empleado lleva a cabo la protección de datos además de otras funciones. De otro modo, las prioridades en conflicto podrían dar lugar al descuido de las obligaciones del DPD. Contar con tiempo suficiente que dedicar a las tareas del DPD es de la máxima importancia. Es una práctica recomendable establecer un porcentaje de tiempo para la función del DPD cuando no se lleve a cabo a tiempo completo. Es también recomendable determinar el tiempo necesario para llevar a cabo la función, el nivel de prioridad apropiado para las funciones del DPD, y para que el DPD (o la organización) redacte un plan de trabajo. 32 Artículo 35(2).

• Apoyo adecuado en cuanto a recursos económicos, infraestructura (locales, instalaciones, equipos) y personal donde sea pertinente. • Comunicación oficial de la designación del DPD a todo el personal para asegurar que su existencia y su función se conozcan dentro de la organización.

• **Acceso necesario a otros servicios,** tales como recursos humanos, departamento jurídico, TI, seguridad, etcétera, de modo que los DPD puedan recibir apoyo esencial, datos e información de esos otros servicios.

• **Formación continua.** Debe darse a los DPD la oportunidad de mantenerse al corriente de todos los avances que se den en el ámbito de la protección de datos. El objetivo debe ser aumentar constantemente el nivel de conocimiento de los DPD, por lo que se les debe animar a participar en cursos de formación sobre protección de datos y otras formas de desarrollo profesional, como participación en foros sobre privacidad, talleres, etcétera.

• **En función del tamaño y la estructura de la organización,** puede que sea necesario establecer un equipo del DPD (un DPD y su personal). En tales casos, la estructura interna del equipo así como las tareas y responsabilidades de cada uno de sus miembros deben delimitarse claramente. Del mismo modo, cuando la función del DPD la ejerza un proveedor de servicios externo, un equipo de personas que trabaje para dicha entidad podrá llevar a cabo de hecho las tareas de un DPD a modo de equipo, bajo la responsabilidad de un contacto principal designado para el cliente. En general, cuanto más complejas o sensibles sean las operaciones de tratamiento, más recursos deberán destinarse al DPD. La función de protección de datos debe dotarse de forma efectiva con recursos suficientes en relación con el tratamiento de datos que se esté llevando a cabo.

5.- ¿Qué diferencias de exigencia y sanciones tiene una empresa privada y una pública con el nuevo reglamento -por ejemplo, a las públicas no se las puede sancionar, qué se hará en este caso?

El nivel de exigencia es el mismo en ambos casos. Con respecto a las sanciones, la actual LOPD incluye un procedimiento denominado de infracción de las Administraciones Públicas encaminado a garantizar el cumplimiento y el seguimiento de las medidas adoptadas por el responsable para dicho cumplimiento. Aunque no incluye sanción, sí declara la infracción e insta a la toma de las medidas correctoras correspondientes.

Por otro lado, la Agencia Española de Protección de Datos ha publicado un documento que contienen un conjunto de medidas que las Administraciones Públicas deberán tener implantadas el 25 de mayo de 2018, fecha en la que será aplicable el Reglamento General de Protección de Datos (RGPD).El documento ‘El impacto del RGPD sobre la actividad de las AAPP’ sintetiza en 15 puntos los aspectos más relevantes que deben estar establecidos cuando el Reglamento sea de aplicación. En muchos casos, los efectos de la nueva normativa van a ser los mismos que para cualquier otro responsable o

encargado pero, en algunas áreas, existen especificidades que deben ser tenidas en cuenta por el sector público.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

6.-Qué tres mitos queréis desmentir desde la Agencia que se están diciendo en foros profesionales...

7.-¿Cómo se protegerá la independencia y ética de un DPD frente a su trabajo en la empresa, ya que puede estar condicionado por ella..?

La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos, entre los que se encuentran:

• Total autonomía en el ejercicio de sus funciones y ausencia de conflicto de interés

• Necesidad de que se relacione con el nivel superior de la dirección

• Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.

8.-¿En qué se diferenciará un DPD de una empresa... de uno externo que se contrate para dar servicio a varias -puede tener que tener acceso a datos personales de clientes de una empresa y no trabajar para ella...-.

El RGPD permite que el DPD mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios. Es decir, permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización. Está permitido que el DPD desarrolle sus funciones a tiempo completo o parcial.

En este último caso, es preciso evitar que existan conflictos de intereses. Estos conflictos pueden surgir cuando el DPD, en su tarea de supervisión de las actividades de tratamiento de datos llevadas a cabo por la organización, debe valorar su propio trabajo dentro de ella, como sucede si se designa DPD al responsable de tecnologías de la información (cuando estas tecnologías se emplean para el tratamiento de datos) o al responsable de un área de negocio que decide sobre determinados tratamientos. El RGPD prevé también el catálogo de funciones del DPD, entre las que se incluyen las relativas a actuar como punto de contacto para los interesados en todo lo que tenga relación con el tratamiento de sus datos personales.

La función del DPD puede ejercerse también sobre la base de un contrato de servicios suscrito con una persona física o una organización ajena a la organización del responsable o el encargado del tratamiento. En este último caso, es esencial que cada miembro de la organización que ejerza las

funciones de un DPD cumpla todos los requisitos pertinentes expuestos en la sección 4 de la RGPD (p. ej., es esencial que nadie tenga un conflicto de interés).

Es igualmente importante que cada miembro que ocupe dicho puesto esté protegido por las disposiciones del RGPD -por ejemplo. que impidan la rescisión injustificada del contrato de servicios por las actividades del DPD así como el despido improcedente de cualquier miembro de la organización que lleve a cabo las tareas de DPD-. Al mismo tiempo, es posible combinar las destrezas y puntos fuertes individuales de forma que varias personas, trabajando en equipo, podrán servir de modo más eficiente a sus clientes. En aras de la claridad legal y la buena organización, se recomienda tener una asignación clara de tareas dentro del equipo del DPD y asignar a una sola persona la función de contacto principal y persona 'a cargo' de cada cliente. Por lo general, también sería útil especificar estos puntos en el contrato de servicios.

9.-¿Estais trabajando para crear un seguro de responsabilidades de DPD con alguna aseguradora o correduría?

Es un trabajo bastante delicado porque si hay una brecha de seguridad profesionalmente puede quedar reputacionalmente arruinado...Como ya se ha indicado, el DPD no es responsable de lo que pueda ocurrir con los tratamientos de datos, en caso de una brecha de seguridad el DPD asesoraría al responsable en su relación con la autoridad de control, o en la manera en la que informar a los interesados pero no ostentaría la responsabilidad. Sería competencia del propio responsable la contratación de un seguro encaminado a paliar las responsabilidades derivadas de una brecha de seguridad. La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos como herramienta útil a la hora de evaluar que los candidatos a ocupar el puesto de DPD reúnen las cualificaciones profesionales y los conocimientos requeridos.

Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por la Entidad Nacional de Acreditación, siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados. La certificación no será un requisito indispensable para el acceso a la profesión, será sólo una opción a disposición de responsables y encargados para facilitar su selección de los profesionales llamados a ocupar el puesto de DPD. Pero responsables y encargados pueden tomar en consideración otras cuestiones u otros medios para demostrar la competencia de los DPD.