

Preguntas de los asistentes

Rafael García Gozalo
Jefe del Departamento Internacional

Empresas que deben tener DPD

El RGPD establece

- Administraciones Públicas
- Tratamiento de datos sensibles a gran escala
- Seguimiento regular y sistemático a gran escala

Decisión corresponde a responsables y encargados tras analizar su situación

Podrían considerarse incluidas en estos criterios, entre otras:

- Entidades aseguradoras y reaseguradoras
- Distribuidores y comercializadores de energía eléctrica o gas natural
- Entidades responsables de sistemas de información crediticia
- Entidades que desarrollen actividades de publicidad que impliquen análisis de preferencias o elaboración de perfiles
- Centros sanitarios
- Centros docentes que ofrezcan enseñanzas regladas, universidades
- Colegios profesionales
- Entidades dedicadas al juego on line...

Procesos de certificación de profesionales

RGPD no establece ningún criterio de titulación para DPD

RGPD requiere

- Cualidades profesionales, en particular, conocimientos especializados del Derecho y la práctica en materia de protección de datos
- Capacidad para desempeñar las funciones

Certificación como instrumento de garantía y transparencia para responsables y encargados, pero no única vía de acceso

- Certificación realizada por entidades certificadoras acreditadas por ENAC

Elaboración del Esquema de Certificación en curso. Esquema será público

Publicación del Esquema supone inicio de procesos de acreditación de entidades certificadoras

AEPD, entidades certificadoras y ENAC monitorizan aplicación del Esquema

Perfil del DPD

Del RGPD se desprende que el DPD ha de ser una persona. No obstante:

- Es posible, y en algunas organizaciones será necesario, que el DPD esté respaldado por una unidad de protección de datos
- Puede haber organizaciones en que sea necesario que existan DPD para ámbitos funcionales o territoriales específicos

En estos casos, debería existir una única persona que sea quien asuma formalmente la posición de DPD

En el caso de DPD con una relación de servicios es posible que el contrato se formalice con una persona jurídica. La recomendación de las autoridades es que haya una persona responsable última dentro de la entidad que presta el servicio

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



www.agpd.es

9ª Sesión Anual Abierta de la Agencia Española de Protección de Datos

Preguntas de los asistentes

Agustín Puente Escobar
Abogado del Estado – Jefe del Gabinete Jurídico

¿Cuál es la incidencia del RGPD sobre la exclusión de los datos de contacto prevista en el artículo 2.2 del RLOPD?

- Los datos de contacto son información referida a personas físicas identificadas (datos de carácter personal) por lo que su tratamiento se encuentra sometido al RGPD.
- En consecuencia no cabe considerar aplicable la exclusión hasta ahora vigente
- El tratamiento deberá cumplir con el RGPD, en particular en lo referente a la legitimación
- Es posible que ese tratamiento se encuentre amparado en la regla de ponderación del artículo 6.1 f) del RGPD si se cumplen los requisitos establecidos en el RLOPD
 - Mínimos datos imprescindibles de contacto
 - Tratamiento con fines de mantenimiento de relaciones B2B

¿Cuáles son las implicaciones del RGPD en relación con el consentimiento?

- El RGPD no implica necesariamente una obligación de recabar un nuevo consentimiento si el que se hubiera obtenido antes de su aplicación fuese conforme a los requisitos que establece (Cdo. 171)
 - Siguen siendo válidos los consentimientos expresos y los consistentes en una manifestación o clara acción afirmativa
 - El Cdo. 32 clarifica supuestos que pueden considerarse consentimiento (declaración, marcación de una casilla, selección de parámetros)
 - En ningún caso hay aplicación retroactiva, dado que las normas del RGPD no se aplican a tratamientos anteriores al momento en que produce plenos efectos
- Cuando se preste el consentimiento para el tratamiento de datos con múltiples finalidades será preciso dar el consentimiento para todos ellos (Cdo. 32). En particular:
 - Consentimientos específicos en el marco de un contrato
 - Consentimientos específicos en el marco de declaraciones

¿Cuáles son las implicaciones del RGPD en relación con el consentimiento?

- En caso de que se recabe el consentimiento para varias finalidades
 - Sería posible agruparlas en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros)
 - Pero deberían desagregarse cuando los tratamientos impliquen conductas distintas (por ejemplo tratamiento por quien recaba los datos y cesión a terceros)
 - En ningún caso la falta de consentimiento podría implicar la denegación de un servicio si el tratamiento no es necesario para su prestación (art. 7.4)
- La aceptación mediante un click de una política de privacidad en que se deja expresamente al interesado la posibilidad de decidir si acepta o no el tratamiento de los datos (a través de casillas no premarcadas – incluso de oposición y no de aceptación-) puede considerarse un consentimiento válido
- En todo caso, el responsable deberá probar que cuenta con el consentimiento y que ha sido prestado por el afectado a través de los medios que resulten pertinentes

¿Cuáles son las implicaciones del RGPD en relación con los supuestos de “consentimiento tácito” que ahora autoriza el artículo 14 del RLOPD?

- Estos consentimientos no resultan conformes al RGPD, por lo que no sería válido persistir en el tratamiento sobre su sola base a partir de 25 de mayo de 2018.
- El período transitorio de adaptación de los consentimientos sería el actual, dado que el RGPD está en vigor pero no es plenamente aplicable.
- Los tratamientos basados en el “consentimiento tácito” deberán encontrar fundamento en otra causa de legitimación
 - Mediante una nueva solicitud del consentimiento
 - Mediante, en su caso, la aplicación de alguna otra causa de legitimación y, en particular, la ponderación del derecho y el interés legítimo del responsable
 - El Cdo. 47 reconoce que el tratamiento con fines de mercadotecnia directa puede considerarse realizado por interés legítimo, aunque deberá ponderarse ese interés con la posible intrusión en el derecho fundamental
- Para determinar si es posible aplicar esta regla habrá de atenderse a las circunstancias de cada tratamiento concreto y, en particular, el origen de los datos, el alcance de la información tratada o la finalidad perseguida, no siendo posible fijar una respuesta única. Por ejemplo
 - Envío de comunicaciones comerciales sobre los propios productos o servicios podría ser adecuada a la vista de la Directiva e-privacy y la LSSI
 - Tratamiento de dato que el afectado hubiese hecho manifiestamente públicos

¿Cómo afecta el RGPD a la información que ha de facilitarse a los afectados?

- Como punto de partida, cuando los datos se recaben con anterioridad a la plena aplicación del RGPD será suficiente la información ya facilitada con arreglo a la LOPD, sin que sea preciso informar nuevamente
- La información debe ser concisa, transparente, inteligible y de fácil acceso. Debe huirse de fórmulas excesivamente legalistas
- Conforme a la “Guía para el cumplimiento del deber de informar” podrá optarse por un sistema de información por capas
 - La primera capa incorporará la información esencial (identificación del responsable, finalidad del tratamiento, ejercicio de derechos, origen de los datos, realización de perfiles)
 - La segunda capa puede encontrarse recogida, entre otros supuestos, en una política de privacidad, que contendrá la totalidad de las exigencias previstas en el RGPD
 - La guía ofrece ejemplos claros sobre el modo de facilitar la información
- Información sobre algunos extremos:
 - Base legal del tratamiento: podría especificarse el fundamento con arreglo al 6.1 del RGPD en la primera capa y su detalle en la segunda (por ejemplo: tratamiento por obligación legal /art. 95 Ley General tributaria)
 - Plazo de conservación: si existieran varios debería indicarse el mayor, que subsume a los restantes

¿Cuál sería el régimen sancionador aplicable tras la plena aplicación del RGPD?

- EL RGPD establece un régimen sancionador que, aun diferente al propio del ordenamiento español, especifica las conductas típicas y las sanciones aplicables.
 - La determinación de conductas típicas nunca podría darse a efectos de tipificación, sino de forma meramente enunciativa, dado que es el artículo 82 del RGPD el que fija en sus apartados 4, 5 y 6 las conductas
 - Del mismo modo, el RGPD establece la posibilidad de imposición de sanciones económicas o (adicional o sustitutivamente) las medidas correctoras establecidas en su artículo 58.2
- No obstante se deja margen a los Estados miembros en determinadas cuestiones
 - Determinación de los plazos de prescripción de infracciones y sanciones
 - Determinación del régimen sancionador aplicable a las Administraciones Públicas.

¿Puede considerarse el Título VIII del RLOPD como metodología de análisis de riesgo?

- El art. 24,1 del RGPD impone la obligación de adoptar medidas técnicas y organizativas adecuadas a “la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa índole y gravedad para los derechos de las personas físicas”
 - El Cdo. 75 enumera algunas de las posibles situaciones de riesgo
- El Título VIII del RGPD dedica la práctica totalidad de su articulado a enumerar las medidas y no a especificar el enfoque basado en el riesgo al que se refiere el RGPD
- Si lo que se plantea es si la división en tres niveles de seguridad efectuada por el artículo 81 del RLOPD es suficiente para valorar el riesgo la respuesta debe ser negativa
 - Este “enfoque” únicamente atiende a la tipología del responsable o de los datos tratados, pero no atiende a los riesgos concretos que pueden afectar a los derechos de las personas ni tiene en cuenta (salvo alguna excepción, como la referida a los datos especialmente protegidos) los riesgos potenciales a los que se refiere el RGPD

¿Cómo afecta el RGPD a las obligaciones de transparencia?

- La legislación de transparencia impone unas obligaciones legales de publicidad o de facilitar a los afectados información solicitada en virtud de su derecho de acceso a información pública
- En consecuencia, las comunicaciones de datos están amparadas en una obligación legal (artículo 6.1 c) del RGPD).
- El artículo 86 del RGPD recoge expresamente esta previsión
- En todo caso, la protección de datos actúa como uno de los límites de transparencia
 - El artículo 15 de la LTAIBG establece la interrelación entre el derecho a la protección de datos y la transparencia
 - Estas normas se completan con los principios contenidos en la legislación de protección de datos
- En consecuencia, el RGPD no introduce ninguna novedad ni limitación nueva en esta materia

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



www.agpd.es

9ª Sesión Anual Abierta de la Agencia Española de Protección de Datos

PREGUNTAS DE LOS ASISTENTES

- **Jesús Rubí Navarrete**
- **Adjunto a la Directora**

Cuando en mayo de 2018 entre en plena aplicación el nuevo Reglamento, los Códigos Tipo existentes, ¿ podrán seguir actuando dentro del territorio español o deberán suspender sus actividades por tener que transformarse en Códigos de Conducta?

- Los Códigos Tipo existentes deben adaptarse al Reglamento Europeo de Protección de Datos para producir los efectos previstos en éste siendo recomendable que incorporen procedimientos extrajudiciales u otros como la mediación para resolver las controversias entre responsables y afectados.

¿Para acceder a la historia clínica de un paciente con el fin de posibilitar la realización de un Proyecto de Investigación determinado, es precisa la autorización específica del paciente en los estudios observacionales retrospectivos, o basta con una autorización genérica al ingreso en el hospital y una aprobación del comité de ética correspondiente?

- Se podría acceder a la historia clínica de los pacientes con la finalidad de hacer un estudio observacional retrospectivo, excluyendo del tratamiento los datos identificativos y contando con la aprobación del comité de ética correspondiente.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



www.agpd.es

9ª Sesión Anual Abierta de la Agencia Española de Protección de Datos