Notas informativas

Resumen del Informe de la Agencia Española de Protección de Datos sobre la utilización de datos biométricos para la realización de pruebas online (10 de mayo 2020)

Protección de Datos Personales – 10 de mayo de 2020

A solicitud de presidente de la CRUE, con fecha 8 de mayo, la Agencia Española de Protección de Datos (AEPD) ha emitido un informe jurídico relativo a la utilización de técnicas de reconocimiento facial con fines de identificación biométrica en los procesos de evaluación online ante la situación de crisis sanitaria ocasionada por el COVID-19. A continuación se ofrece un resumen de su contenido.

I. Consideraciones previas

Comienza la AEPD destacando dos cuestiones:

1. La situación actual no implica la suspensión del derecho fundamental a la protección de datos, por lo que todo tratamiento de datos personales debe ajustarse a las previsiones del Reglamento General de Protección de Datos (RGPD).
2. La realización de evaluaciones online no es algo novedoso ni generado por el estado de alarma, sino que se trata de un método de evaluación que viene aplicándose por algunas universidades españolas desde hace años, empleándose para la identificación, métodos alternativos al reconocimiento facial, como la asignación de identificadores de acceso o el empleo de herramientas de videoconferencia o webcams. Ahora bien tratándose del empleo de técnicas de reconocimiento facial que implican una mayor intrusión en el derecho a la protección de datos personales, y existiendo medidas alternativas, debe primar un criterio de prudencia, siendo necesario un riguroso estudio de los riesgos que implican esos tratamientos y de las garantías necesarias para proteger el derecho a la protección de datos personales, siendo necesario realizar los correspondientes análisis de riesgos, evaluaciones

de impacto y, en su caso, consulta previa a la autoridad de control.

II. Licitud del tratamiento de datos personales en la evaluación del estudiantado

Con carácter general, los tratamientos de datos personales derivados de la necesaria evaluación del estudiantado se encuentran amparados por el artículo 6.1.e) del RGPD, esto es, se trata de tratamientos de datos necesarios para el cumplimiento de una misión realizada en interés público, derivada de una competencia atribuida por una norma con rango de ley conforme al artículo 8.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derecho digitales (LOPDGDD). En concreto, es una competencia de las universidades derivada la configuración de la educación superior como un servicio público (artículo 1.1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades –LOU-). En cualquier caso, como en cualquier tratamiento de datos personales, deben respetarse los principios relativos a la protección de datos recogidos en el artículo 5 del RGPD. Así se ha recogido anteriormente por la AEPD en sus informes 30/2019 (publicación de las calificaciones de los alumnos) y 63/2019 (grabación de los exámenes orales o de sesiones docentes).

Ahora bien, advierte la AEPD, la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador (apartados 2 y 3 del artículo 6 RGPD), así como a los principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos.

Y, además, en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, como sucede con los datos biométricos, será necesario que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición general de tratamiento de dichos datos.

Referida la consulta a la utilización de técnicas de reconocimiento facial para la identificación del estudiante, el tratamiento afecta a datos biométricos definidos por el RGPD como «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos» (art. 4.14 RGPD). Este concepto abarca tanto la identificación biométrica (proceso de comparar datos biométricos, adquiridos en el momento de la identificación, con una serie de plantillas biométricas almacenadas en una base de datos (correspondencias uno-a-varios), como la verificación/autenticación biométrica (proceso de comparación entre datos

biométricos, adquiridos en el momento de la verificación, con una única plantilla biométrica almacenada en un dispositivo (correspondencias uno-a-uno).

Con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en el supuesto de la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno). Es decir, se estará ante un tratamiento de datos de categoría especial sólo en el caso de que tales datos se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física (artículos 4.14 y 9.1 RGPD). Así resulta también del Considerando 51 RGPD: «El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física».

Los sistemas e-proctoring existentes en el mercado implican tratamiento de datos de categoría especial, dado que garantizan la identificación del alumno mediante el reconocimiento facial, evitando la suplantación de su identidad, no solo en el momento inicial, sino a lo largo del desarrollo de toda la actividad, para lo cual se graba la misma y se van realizando diferentes capturas que se comparan con la información biométrica previamente almacenada en sus bases de datos. Asimismo, dichos sistemas pueden incluir el tratamiento de otro tipo de datos biométricos (como las pulsaciones en el teclado) y de datos no biométricos, como la grabación del entorno en el que se encuentra el alumno, así como el acceso al micrófono para la grabación de sonidos. En este sentido, concluye la AEPD que, atendiendo a las circunstancias concretas, los procesos de reconocimiento facial empleados para la realización de evaluaciones online implican el tratamiento de datos biométricos con la finalidad de identificar unívocamente a una persona física.

La regla general contenida en el artículo 9.1 RGPD es la prohibición de tratamiento de datos de categoría especial: datos personales que revelen las opiniones políticas, revelen el origen étnico o racial, las convicciones religiosas o filosóficas o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. No obstante, se autoriza el tratamiento de todos esos datos cuando concurra alguna de las diez circunstancias mencionadas en el apartado 2 del artículo 9 del RGPD. En particular, la AEPD analiza dos de las excepciones que pueden resultar aplicables a la consulta planteada: la posibilidad prevista en la letra a) de la norma, esto es, que el estudiante pudiera prestar su consentimiento al tratamiento y en qué medida dicho consentimiento podría considerarse libre; y la establecida en la letra g), la existencia de un interés

público esencial.

A. Consentimiento del estudiante.

En cuanto a la utilización del consentimiento como base legal para utilizar el reconocimiento facial, el RGPD establece que el consentimiento del afectado debe ser libre y que no puede considerarse prestado de forma libre y, por tanto, válida cuando el afectado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno. Tampoco puede considerarse libre cuando existe un desequilibro claro entre el interesado y el responsable del tratamiento. Partiendo de dichos criterios, la posibilidad de admitir un consentimiento libre de los estudiantes que permitiera el empleo de técnicas de reconocimiento facial para tratar sus datos biométricos en las evaluaciones online requeriría que a los mismos se les ofreciera la posibilidad de realizar dichas evaluaciones en una situación equiparable en la que no fuera necesario su tratamiento, como pudiera ser la realización de la misma actividad presencialmente, u ofreciendo otras alternativas que no requieran el tratamiento de sus datos biométricos y que fueran equiparables en cuanto a su duración y dificultad respecto a las que se realicen con reconocimiento facial. En otro caso como, por ejemplo, si las actividades alternativas ofrecidas fueran más gravosas o implicaran una mayor dificultad, el consentimiento no podría considerarse libremente prestado. Y lo que no sería admisible, en ningún caso, es que como consecuencia de la denegación del consentimiento se denegara la posibilidad de matriculación o de acceder a la evaluación o cualquier otra consecuencia negativa importante para el alumno. El informe añade que corresponde a las universidades, en virtud del principio de autonomía universitaria y como responsables del tratamiento, determinar en sus normas de evaluación y en sus planes de formación los procedimientos de evaluación que acrediten la igualdad entre los alumnos que consientan el tratamiento de sus datos biométricos y los que no lo hagan. Sólo así el tratamiento podría estar basado en el consentimiento.

B. Interés público esencial.

Por otro lado, el tratamiento de datos personales necesarios para la prestación del servicio público de educación se legitima, con carácter general, en la existencia de un interés público. Sin embargo, en el caso del reconocimiento facial, al tratarse de categorías especiales de datos, el RGPD requiere la existencia de un “interés público esencial” para que pueda ser legítimo, profundizando así en la importancia y necesidad de mayor protección de los datos tratados.

La aplicación del interés público esencial como base de legitimación requiere de una norma con rango de ley que justifique en qué medida y en qué supuestos la

identificación de los estudiantes mediante el empleo de la biometría respondería a tal interés público esencial. En este sentido, el artículo 46.3 LOU referido al establecimiento por las universidades de procedimientos de verificación de los conocimientos de los estudiantes se considera insuficiente para permitir la utilización de técnicas de reconocimiento facial en los procesos de evaluación. No existe en la actualidad en el ordenamiento jurídico tal norma con rango de ley que, además, exigiría una especial justificación de la necesidad de optar por el reconocimiento facial respecto otras medidas que permiten acreditar la identidad de los alumnos y supervisar los procesos de evaluación con una menor intrusión en los derechos de los afectados, definiendo asimismo las garantías técnicas, organizativas y procedimentales adecuadas, y respetando el principio de proporcionalidad y el juicio de necesidad (que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia).

Es en relación con este último aspecto, en el que podría tener una especial incidencia la situación generada como consecuencia del Covid-19 y de la declaración del estado de alarma, en la que podría valorarse la prevalencia del reconocimiento facial frente a otras medidas, atendiendo a que la medida consistente en la evaluación presencial pudiera no ser posible, tal y como ocurre en el momento actual. Ahora bien, a juicio de la AEPD, no debe optarse por tal medida con carácter general, sino que debería quedar limitada a aquellas enseñanzas y asignaturas concretas que, por su importancia, complejidad u otras circunstancias de especial incidencia, no aconsejaran acudir a otras opciones, como la evaluación continua, o hicieran excesivamente gravoso la adopción de otros medios como el control por videocámara o la realización de exámenes orales.

III. Análisis de riesgos y garantías necesarias en los tratamientos de datos biométricos

Por último, advierte la AEPD que tanto en el caso de que se procediera al reconocimiento facial sobre la base de un consentimiento libre de los afectados como en el caso de que se apruebe una norma con rango de ley que lo ampare conforme al artículo 9.2.g), deberán adoptarse todas las medidas que garanticen que el tratamiento es conforme a la normativa sobre protección de datos personales, las cuales, en el último caso, deberán recogerse en la propia norma legal, sin perjuicio de su especificación por el responsable.

Para la adopción de tales medidas resultará esencial la realización del correspondiente análisis de riesgos (artículo 24 RGPD), a lo que se añade la necesidad de realizar una evaluación de impacto de datos (artículo 35 RGPD). Asimismo, se deberá consultar a la autoridad de protección de datos competente antes de proceder al tratamiento cuando la evaluación de impacto muestre que el

tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo (artículo 36 RGPD), salvo que el responsable sea capaz de garantizar que el riesgo puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación (Considerando 94 RGPD). En el supuesto de que el tratamiento se vaya a realizar por un tercero por cuenta de la universidad (encargado del tratamiento) existe el deber de seleccionar uno que ofrezca garantías suficientes y haberse suscrito un contrato con el contenido del artículo 28 RGPD. Asimismo, deberán adoptarse las medidas de seguridad necesarias conforme a lo previsto en el artículo 32 RGPD, teniendo en cuenta el Esquema Nacional de Seguridad, aplicable solo a las universidades públicas, y las medidas a adoptar que resulten del correspondiente análisis de riesgos.

Para consultar el informe completo pulse aquí: • Informe 0036-2020 de la Agencia Española de Protección de Datos sobre la utilización de datos biométricos para la realización de pruebas online

Resumen del Comunicado Comisión Europea sobre protección de datos en las aplicaciones móviles de apoyo a la lucha contra la pandemia COVID-19 (Protección de Datos Personales (20 de abril de 2020))

Recientemente la Comisión Europea ha emitido el comunicado (2020/C 124 I/01) relativo a orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia COVID-19, en lo referente a la protección de datos, con vistas a que, desde los Estados Miembros de la Unión, se aborde un enfoque europeo que proporcione a los ciudadanos mecanismos que limiten la propagación del COVID-19 con garantías para la intimidad y la protección de los datos personales.

En este sentido, la interrupción de las cadenas de infección con mayor celeridad y de forma efectiva por medio de **aplicaciones** pueden contribuir **en la fase de desescalada** hacia una nueva normalidad con un menor riesgo de propagación significativa del virus.

Las orientaciones que a continuación se reseñan y que no son jurídicamente vinculantes, se han elaborado con las contribuciones efectuadas tanto por el Comité Europeo de Protección de Datos como por los debates producidos en la red de sanidad electrónica (eHealth).

En primer lugar, las aplicaciones móviles de apoyo que se desarrollen en la lucha contra la pandemia deben incardinarse en **UNA DE LAS SIGUIENTES FUNCIONALIDADES**

con sus particularidades:

- **Facilitar información sobre la pandemia**
- **Rastreo de contactos y alerta**
- **Comprobación de síntomas y telemedicina**

En segundo lugar, la Comisión considera, en atención al derecho a la confidencialidad de las comunicaciones y en base a un juicio de proporcionalidad, adecuación y necesidad, que **EL USO DE LAS APLICACIONES SEA DE CARÁCTER VOLUNTARIO**, no debiendo constituir, por el alto grado de intrusión y la complejidad en cuanto al establecimiento de salvaguardas, una imposición al usuario.

Así pues, no se contemplan en estas recomendaciones las aplicaciones destinadas a controlar el grado de cumplimiento de las obligaciones de cuarentena.

Tras detallar la repercusión y contribución que las distintas funcionalidades de aplicaciones de apoyo presentan, SE ESTABLECEN UNA SERIE DE RECOMENDACIONES:

- Se aconseja que el diseño de las mismas ha de contemplar que **las autoridades sanitarias nacionales sean las responsables del tratamiento de los datos**, lo que estimularía la confianza de los ciudadanos en cuanto a su uso. En este sentido, estima que **el ciudadano ha de apreciar que posee el control de sus datos personales**, sugiriendo que **la instalación sea de carácter voluntaria** sin que exista consecuencia negativa alguna si se decide no instalarla o tras hacerlo si se desinstala.
- Del mismo modo, **las distintas funcionalidades de la aplicación no deberían agruparse**, aunque ha de mantenerse la opción, para que la persona sea quien decida si da su consentimiento específicamente a cada una de ellas y, **en el caso de que se utilicen, datos de proximidad** (señales de Bluetooth de baja energía (BLE)), éstos **han de almacenarse en el dispositivo del usuario**.
- La **comunicación de datos a las autoridades sanitarias** debería de hacerse tras confirmar **que la persona** está infectada de COVID-19 y cuando ésta **opte porque se haga de esta manera**.
- Las autoridades sanitarias han de proporcionar la información respecto del tratamiento de datos personales al **interesado** y éste **ha de poder ejercer sus derechos, sobre todo los de acceso, rectificación y supresión.**
- Finalmente, **cuando la pandemia esté controlada** las aplicaciones deberían **desactivarse**, no condicionado este aspecto a la desinstalación por los usuarios.

¿Cuál es la base jurídica para el tratamiento de los datos?

Instalación de aplicaciones y almacenamiento de información enel dispositivo del usuario.

La Comisión considera que la base jurídica para el tratamiento **puede fundarse en dos motivos**:

- Que el almacenamiento o acceso **sean necesarios para el servicio** de la sociedad de la información **que el usuario ha solicitado de manera expresa** o
- Que el usuario **haya dado su consentimiento libre, específico, inequívoco e informado.**

En el supuesto de que la carga de ciertos datos no sea necesaria para el funcionamiento en sí de la aplicación, deberá ajustarse a uno de los motivos expuestos.

Autoridades sanitarias nacionales

La base jurídica para el tratamiento de datos se funda **en la existencia de una obligación legal** de conformidad con el artículo 6.1 c) RGPD o **por ser necesario para la realización de una misión de interés público** de acuerdo al artículo 6.1 e) RGPD, ambos en consonancia con el artículo 9, apartado 2, letra i) del mismo cuerpo normativo para el tratamiento de **datos de categorías especiales.**

¿Se protegen los datos de carácter personal?

Los datos que se generan y se almacenan gozan de la cobertura que el Reglamento General de Protección de Datos proporciona, especialmente los datos de salud.

Los datos vinculados a la localización y posición geográfica de terminales móviles se encuentran protegidos por la Directiva sobre privacidad y comunicaciones electrónicas.

¿Qué tipo de datos se requieren según la funcionalidad de la aplicación?

Facilitar información sobre la pandemia

No requerirá tratamiento de **datos personales**.

Rastreo de contactos y alerta

Se recomienda que se traten **datos de proximidad** (BLE) **y no datos de geolocalización**, ya que los primeros impiden el rastreo y los de localización no son

necesarios a estos fines.

Sólo deberían generarse **datos de proximidad si existe riesgo real de infección** , de forma que el almacenamiento del momento y el lugar de contacto no sería proporcional o necesaria, sobre todo si con saber el día de contacto se cumple con la finalidad del tratamiento.

Comprobación de síntomas y telemedicina

Se precisan datos de salud, en lo que respecta al **número de teléfono de contacto** del usuario, ha de ser proporcionado por éste. Las autoridades sanitarias nacionales han de **elaborar un listado de los datos que posiblemente hayan de tratarse**.

¿Existen límites a la divulgación y acceso a los datos?

Facilitar información sobre la pandemia

No se puede compartir con autoridades sanitarias ninguna información almacenada en el terminal y a la que se acceda desde el equipo.

Rastreo de contactos y alerta

Hay que **distinguir** entre los **datos de personas infectadas** y los **datos de personas que han estado en contacto con la persona infectada**.

1. En el primer caso, se recomienda que **los identificadores de rastreo se almacenen en el dispositivo del usuario**, al estar acorde con el principio de minimización. Otra alternativa, es que **se almacenen en un servidor al que las autoridades sanitarias tengan acceso tras haber sido compartido de forma proactiva con ellas**. No debería de ser informado de las personas con las que ha podido tener contacto epidemiológico.
2. En el segundo caso, **la persona que ha estado en contacto con una persona infectada, no debería conocer la identidad de ésta**, resultando suficiente la comunicación del posible contacto en los últimos dieciséis días, **sin especificar datos del momento ni el lugar**, ni tampoco almacenarlos o comunicarlos.

En todo caso, las autoridades sanitarias nacionales deberían ser informadas del identificador de las personas que han tenido contacto epidemiológico con infectados desde cuarenta y ocho horas antes de la aparición de síntomas hasta catorce días después de su aparición.

Igualmente, el **Centro Europeo para la Prevención y el Control de Enfermedades** puede **recibir datos agregados** por parte de las autoridades

nacionales a los sólo efectos de vigilancia epidemiológica.

Comprobación de síntomas y telemedicina

Es factible que **autoridades sanitarias** competentes y epidemiológicas nacionales **puedan tener acceso a la información procurada por el usuario**. En cuanto a telemedicina se refiere, **el usuario puede decidir revelar a las autoridades sanitarias el número del móvil para que el contacto se produzca con los agentes sanitarios**, procurando que no se produzca el contacto a través de la aplicación.

¿Cómo han de tratarse los datos?

De conformidad con los principios del artículo 5 del RGPD, los datos se tratan de forma adecuada y pertinente, en relación con los fines precisos para los que se recaban y en consonancia con la funcionalidad de la aplicación, limitando los plazos de conservación y garantizando la minimización de los datos, así como su veracidad y exactitud, basándose en tecnologías que permitan una evaluación más precisa de los contactos.

¿Cuáles son los fines por los que se tratan datos de carácter personal?

Depende de las funcionalidades de la aplicación y han de especificarse:

Facilitar información sobre la pandemia

Proporcionar información pertinente para las autoridades sanitarias en el contexto de la crisis epidemiológica.

Rastreo de contactos y alerta

Considera la Comisión que no es suficiente con indicar como finalidad “la prevención de nuevas infecciones de COVID-19”, especifica para una mayor concreción que se establezca como finalidad la de: **“mantener los contactos de las personas que utilizan la aplicación y que pueden haber estado expuestas a la infección de la COVID-19 con el fin de alertar a aquellas que podrían haber sido infectada”**.

Comprobación de síntomas y telemedicina

- Ofrecer al usuario, a través de cuestionarios para su auto-cumplimentación o una serie de preguntas, valorar el desarrollo de síntomas de la COVID-19 o proporcionar al usuario asesoramiento médico si han desarrollado los síntomas de la COVID-19

¿Existen límites para el almacenamiento de datos?

Sí, no deberían almacenarse más tiempo del **estrictamente necesario** en atención a la importancia de la situación sanitaria.

Facilitar información sobre la pandemia

Supresión inmediata, no se precisan datos para aplicaciones con esta funcionalidad.

Rastreo de contactos y alerta

Los datos de proximidad **han de suprimirse tan pronto dejen de ser necesarios para alertar a los usuarios**. Deberían suprimir en un período **máximo de un mes** o **tras** haber dado la persona un **resultado negativo** en las pruebas a las que se someta. Por su parte, las autoridades sanitarias nacionales podrán conservarlos durante períodos más largos a efectos de información sobre vigilancia e investigación si se hace en formato anonimizado.

Se han de **almacenar los datos en el dispositivo del usuario salvo los que hayan sido comunicados por usuarios** y que siendo necesarios para la finalidad, se hayan cargado en el servidor a disposición de las autoridades sanitarias cuando así se haya optado.

Comprobación de síntomas y telemedicina

Los datos habrán de suprimirse, como indica la Comisión, **en un período máximo de un mes o tras haber dado la persona un resultado negativo en las pruebas a las que se someta**. Se podrán conservar por un período más largo otros datos de forma anonimizada a efectos de informar sobre vigilancia e investigación.

¿Qué aspectos de seguridad han de contemplarse?

Datos almacenados en terminales: cifrados con las técnicas criptográficas más avanzadas.

Datos almacenados en servidores: el acceso, incluido el administrativo, sometido a registro previo.

Datos de proximidad: sólo generarse y almacenarse en el terminal del usuario, en formato cifrado y pseudonimizado, la activación del Bluetooth ha de ser independiente a la activación de otros servicios de localización. En la recogida de datos, ha de crearse y almacenarse identificadores temporales del usuario que cambien periódicamente y no el identificador real del terminal.

Código fuente: que se haga público y se encuentre disponible para su revisión.

Las transmisiones desde el dispositivo a autoridades nacionales han de estar cifradas, adoptándose medidas adicionales como la anonimización o supresión automática tras un transcurso de plazo determinado. Si se contempla el uso compatible de los datos con fines de investigación científica, habrá que recurrir a la pseudonimización.

Se recomienda, que las autoridades de protección de datos participen y sean consultadas en el desarrollo de la aplicación, en particular en lo relativo al tratamiento de datos a gran escala y la necesidad de realizar una evaluación de impacto.

- Para consultar o descargar el informe completo pulse aquí.

Resumen del Informe de la AEPD 2019-0036 sobre tratamientos de datos en el ámbito universitario (Protección de Datos Personales - 15 de octubre de 2019)

La Agencia Española de Protección de Datos (AEPD) ha emitido un informe jurídico en el que responde a variadas cuestiones relativas al tratamiento de datos personales en el ámbito universitario.

1. Cesiones de datos relativos a las cantidades abonadas en concepto de complemento de productividad y gratificaciones por servicios prestados fuera de la jornada normal de trabajo, así como a las indemnizaciones por razón del servicio (dietas) abonadas a personal de la universidad.

La AEPD considera, conjuntamente con el Consejo de Transparencia y Buen Gobierno, que el sector público estatal tiene la obligación de facilitar información sobre las relaciones de puestos de trabajo y retribuciones, ya sea por el ejercicio del derecho de acceso a la información pública o como publicidad activa.

Mantiene que las cantidades del complemento de productividad son de conocimiento público para quienes dependen de la Administración General del Estado, conforme al artículo 23.3 c) de la Ley 30/1984, de 2 de agosto, de medidas para la reforma de la Función Pública.

No obstante, la comunicación a los representantes sindicales, al haber sido derogado tácitamente el último inciso del citado precepto por el artículo 40 de la Ley 7/2007, de 12 de abril del Estatuto Básico del Empleado Público, no será procedente.

En todo caso, la publicidad de la productividad no debe dar lugar, con su acceso, a tratamientos posteriores que puedan resultar contrarios a lo dispuesto en la legislación de protección de datos o genere situaciones que puedan poner en riesgo los derechos de los empleados.

Para el caso de las universidades privadas, la publicación podría estar amparada en la base legal del artículo 6.1.f) Reglamento General de Protección de Datos (RGPD), siempre que responda a una finalidad legítima de la universidad, como podría ser incentivar la productividad de sus trabajadores, así como a un interés legítimo de los propios empleados, que de este modo, podrían conocer su propio rendimiento en comparación con el resto de compañeros, garantizándose la transparencia de este dato.

La cesión a terceros de datos relativos a la productividad, gratificaciones o dietas al margen de los supuestos descritos, precisará del consentimiento de los afectados sin que pueda justificarse el tratamiento sobre la base de un interés público.

Igualmente sucede con los gastos asociados a un determinado proyecto, así como con las indemnizaciones por razón del servicio de los investigadores pertenecientes al grupo de investigación en el que se enmarca cada proyecto, en el marco de los contratos del artículo 83 Ley Orgánica de Universidades.

En cualquier caso, toda publicación deberá realizarse de modo que resulte lo menos perjudicial para el interesado.

2. Publicación de la producción científica del personal investigador

El artículo 37 de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, en cuanto a la publicación de la producción científica del personal investigador, establece lo siguiente:

“El personal de investigación cuya actividad investigadora esté financiada mayoritariamente con fondos de los Presupuestos Generales del Estado hará pública

una versión digital de la versión final de los contenidos que le hayan sido aceptados para publicación en publicaciones de investigación seriadas o periódicas".

De la norma deriva la existencia de una obligación legal conforme el artículo 6.1. c) del RGPD que legitima su publicación. Ante estos supuestos, no procederá el ejercicio del derecho de oposición previsto en el artículo 21 RGPD al no poder fundamentarse en la existencia de interés público o interés legítimo.

Para el tratamiento respecto a índices de calidad como el ranking por citación o los informes bibliométricos realizados a nivel institucional, al no existir una obligación legal como en el caso anterior, podría encontrase amparado en la existencia de un interés público cuando una ley formal así lo prevea. Si no existiese ley formal, se requerirá el consentimiento del afectado.

La publicación de evaluación de tramos de investigación, las encuestas realizadas por alumnos sobre calidad docente, así como las acreditaciones para acceso a distintas categorías profesionales de profesorado, se encuentran amparadas en la existencia de un interés público de acuerdo con lo previsto en la letra e) del artículo 6.1 del RGPD, ya que según la Ley Orgánica de Universidades, para la búsqueda de la mejora de la calidad del sistema universitario y desarrollo de la de educación superior, se precisa la mejora de la gestión y visibilidad de la investigación. Por tanto, podría procederse a la publicación siempre que las normas internas de cada universidad concreten el procedimiento de elaboración de los índices, de tal manera que se previera dicha publicación, hecho que podría amparar el tratamiento en el artículo 6.1.b) del RGPD.

3. Acceso a los datos académicos de cargos públicos y a la publicación de dichos datos en el portal de transparencia de las universidades

Procederá el acceso a datos de cargos de la propia Universidad siempre que, se realice conforme a los supuestos contemplados en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG) y aplicando las cautelas que en la misma se establecen, especialmente lo previsto en su artículo 15, y de conformidad a lo señalado en los criterios interpretativos conjuntos que puedan adoptar el Consejo de Transparencia y Buen Gobierno y la AEPD.

4. Acceso a los contenidos de los trabajos (de fin de grado, de fin de máster o de tesis)

La publicación de datos contenidos en tesis doctorales, examinando lo dispuesto por

los artículos 11.2, 13.3 y 14.5 del Real Decreto 99/2011, de 28 de enero, por el que se regulan las enseñanzas oficiales de doctorado, se encuentra amparada en el artículo 6.1 b) del RGPD. Resulta así, debido a que los doctorandos se someten al régimen jurídico contractual del programa de Doctorado, del que se surgen obligaciones relativas a la publicidad por parte de las Universidades, de tal forma que se garantice que otros doctores puedan realizar observaciones durante los procesos de evaluación y que exista constancia, una vez defendida, en los repositorios institucionales con la información complementaria necesaria por el Ministerio de Educación.

Para los trabajos de fin de grado y fin de máster, dado que no existe norma similar a nivel estatal, se deberá acudir a la normativa específica de cada universidad para comprobar si resulta procedente su tratamiento conforme a un régimen jurídico establecido o contractual del programa. De no ser así, se debe recabar el consentimiento del afectado.

Si la solicitud de acceso proviene del ejercicio de acceso a la información pública de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, deberá aplicarse lo dispuesto en su artículo 15.

5. Acceso de los progenitores a las calificaciones de sus hijos, económicamente dependientes

La AEPD mantiene que, de ser apreciable un interés legítimo al amparo de lo previsto en el artículo 6.1.f), se podría facilitar ésta información. Para ello habría que realizar un análisis acerca de si el tratamiento de los datos es necesario para satisfacer el interés legítimo que se alegue, a la vez que se efectúa una ponderación acerca de si ha de prevalecer dicho interés sobre el derecho fundamental a la protección de datos del interesado.

En el caso de que el obtener las calificaciones académicas de hijos/as mayores de edad, tenga como finalidad exclusivamente la de utilizarlas en un procedimiento judicial para la solicitud de modificación de la pensión de alimentos, prevalecerá el interés legítimo sobre el derecho a la protección de datos, sin que exista la posibilidad de ejercitar el derecho de oposición. Resulta fundamental analizar cada caso concreto, de tal manera que, si existe abono de pensión alimenticia o dependencia económica se podrá presumir la existencia de interés legítimo.

Por otro lado, si se tratase de menores de edad no emancipados o declarados incapaces judicialmente, será oportuna la facultad de acceso a la información en tanto que la obligación de educación de los progenitores hacia sus hijos lo ampara.

Se recomienda antes de resolver la solicitud, valerse del trámite de audiencia al

afectado, que aunque no se contempla en la normativa de protección de datos, constituye una buena práctica. Si el acceso se solicita en base al derecho de acceso a la información pública y buen gobierno deberá darse dicho trámite de audiencia al amparo del artículo 19.3 LTAIBG.

De acuerdo a lo expuesto, a la hora de ponderar la solicitud, se recomienda requerir el último ingreso abonado antes de la solicitud además de la resolución judicial, para determinar que no se ha dejado de satisfacer las pensiones alimenticias.

6. Grabación y divulgación de imágenes en actos públicos organizados por la Universidad

La captación y divulgación de imágenes de actos públicos organizados por Universidades, cuando se trate de imágenes accesorias o accidentales, se encuentra amparada en la letra e) del artículo 6.1 del RGPD, al ser una misión de interés público en consonancia con la promoción de la actividad universitaria en las diferentes esferas de actuación descritas en la Ley Orgánica de Universidades.

En el caso de difusión de imágenes captadas cuando afecten a personas que ejerzan un cargo público o profesión de notoriedad o proyección pública se estaría ante un interés público del artículo 6.1 e) RGPD amparado en el artículo 8.2 a) de la LO 1/1982 de 5 de mayo, sobre protección civil, del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En los restantes supuestos, será preciso el consentimiento inequívoco de las personas cuyas imágenes son objeto de captación y posterior divulgación, debiendo cumplirse con el deber de informar previsto en el artículo 13 del RGPD, que deberá incluir los fines del tratamiento a que se destinan los datos personales.

7. Grabación de exámenes orales y de las sesiones de docencia

La grabación de exámenes orales precisa, para que sea legítima conforme a la normativa de protección de datos, que se encuentra amparada en una base legal para el tratamiento.

Si bien existen medios menos intrusivos para la privacidad, cuando la grabación esté encaminada a la obtención de un medio de prueba para que los alumnos puedan ejercer su derecho a revisión y para que los docentes puedan justificar la evaluación, siempre y cuando conforme a los Estatutos y normas de organización y funcionamiento que regulen estos procedimientos se prevean, el tratamiento será necesario para el cumplimiento de una misión realizada en interés público conforme al artículo 6.1 e) RGPD.

En el caso de las grabaciones de sesiones de docencia, la AEPD distingue en función de si el interesado en la grabación es un estudiante o un docente: • En el primer supuesto, la base que legitima la grabación por parte de un estudiante de una sesión de docencia, será el consentimiento, 6.1a) RGPD, que deberá recabar previamente del resto de estudiantes y el profesor. • Si la grabación es realizada por el profesor, siempre y cuando se efectúe exclusivamente en el ejercicio de la función educativa, no requerirá previo consentimiento de los asistentes a clase y será conforme al artículo 6.1 e) RGPD de acuerdo con la Ley Orgánica de Universidades.

Conviene advertir que, conforme a la citada finalidad, no se prevé la divulgación y la accesibilidad, ésta última, sólo podrá tener lugar con el consentimiento expreso de los participantes en dicha actividad y el profesor.

Si es la Universidad la que, con fines de control laboral, realiza grabaciones, el fundamento se encontraría en el artículo 6.1 b). RGPD.

8. Acceso a los datos de personas fallecidas, como podría ser la cuenta profesional de correo electrónico o las calificaciones académicas

La AEPD ha venido defendiendo que el derecho a la protección de datos, en cuanto derecho de la personalidad, se extingue por la muerte de la persona conforme al artículo 32 del Código Civil. Si bien, conforme al artículo 3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de y garantía de los derechos digitales (LOPDGDD), los afectados tienen plena disposición sobre sus datos, puede haber prohibido el ejercicio de los derechos respecto a sus datos o haber designado a personas o instituciones que podrán ejercitarlos de acuerdo con sus instrucciones. En los casos en que no hayan expresado esta voluntad, se reconoce legitimación para actuar a cualquier persona vinculada por razones familiares o de hecho, así como a quienes resulten ser herederos.

No obstante, la intervención de los herederos, en cuanto al acceso a los datos del causante, sólo tendrá amparo conforme a la LO 1/1982, para proteger su memoria o en defensa de su derecho hereditario. En este sentido, tales accesos no podrán ser

considerados como manifestaciones del derecho de acceso.

Aunque el derecho a la intimidad del fallecido se extinga con su muerte, puede subsistir el derecho a la intimidad de las terceras personas que se relacionaban con él o incluso, de aquellos que fueran citados en sus informaciones o mensajes.

Del mismo modo, el uso de cuentas profesionales de correo electrónico implica el uso de una herramienta de titularidad de la Universidad destinada a fines estrictamente laborales. Por tanto, el acceso al contenido de la cuenta de correo electrónico profesional de una persona fallecida, por quien acredite ser su heredero o heredera, no se facilitará cuando existan datos de terceras personas en los contenidos de los correos. En lo que respecta a calificaciones académicas o historiales administrativos, en base a lo previsto en el artículo 3 LOPDGDD, se facilitará el acceso, salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

9. Cesión de datos a organizaciones sindicales y representantes de los trabajadores

La amplitud de la casuística en cuanto a comunicaciones de datos a organizaciones sindicales y representantes de los trabajadores exige que se analice caso por caso, en atención a lo que disposiciones legales o convenios colectivos puedan establecer conforme indica el artículo 88.1 del RGPD.

Será fundamental que las comunicaciones, a los representantes de los trabajadores pertenecientes a la representación sindical, de datos que resulten procedentes en la medida en que sean necesarios, bien para la negociación de las condiciones de trabajo de los trabajadores representados, bien para la emisión de informes, bien para informar a los trabajadores, o bien para ejercer el control de legalidad, se produzcan de forma disociada sin poder referenciar los datos a personas identificadas o identificables y atendiendo a los principios expuestos en el artículo 5.1 RGPD. En caso contrario, deberá recabarse el consentimiento de los interesados.

De existir esta obligación con motivo de una norma legal que la ampare, la legitimación vendrá dada por el artículo 6.1 c) RGPD.

En cuanto a las facultades de vigilancia o control, si se refieren a un sujeto concreto que haya formulado una queja ante el órgano de representación, será posible la cesión de los datos específicos de dicha persona. En los demás supuestos, la cesión al órgano de representación de información debidamente disociada, cumplirá con la finalidad de la función de control.

Las comunicaciones relativas a nóminas, en los supuestos que el Convenio Colectivo

de aplicación contemple la cesión de dicha relación, podrá fundamentarse en el artículo 6.1 b) del RGPD, siempre y cuando se atienda al principio de minimización y limitación de la finalidad.

En el caso de cesión de los datos de trabajadores laborales, únicamente podría entenderse amparada en caso de que se produjera en el ámbito de las funciones desarrolladas por los Delegados de Personal o el Comité de Empresa, al encontrarse reconocido por el Estatuto de los Trabajadores el derecho de los representantes de los trabajadores (Delegados de Personal o Comité de Empresa) a acceder a determinados datos de los trabajadores en el ámbito de sus competencias. En caso contrario, será necesario el consentimiento del interesado para proceder a la comunicación de sus datos

Los datos de la relación o catálogo de puestos de trabajo que consistan únicamente en aquellos que deban figurar en éstas junto con el nombre y apellidos de la persona que ocupa dicho puesto, no son más que datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano (art. 15.2 LTAIBG), y en atención al derecho de las personas interesadas a identificar al personal que tramita los respectivos procedimientos conforme al art. 53.1.b de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. El tratamiento se encuentra amparado en el artículo 6.1 c) RGPD.

10. Investigaciones que se enmarcan en proyectos de investigación institucionales desarrolladas por universidades o centros públicos de investigación en ámbitos no relacionados con el campo de conocimiento de la salud

Determinar qué base aplicable legitima el tratamiento de datos personales dependerá del caso concreto y de la existencia de normativa especial aplicable.

En cualquier caso, siempre y cuando en la investigación se traten categorías especiales de datos, habrá que tener en cuenta que, el artículo 9.2. j) RGPD, permite levantar la prohibición de su tratamiento conforme a lo que se establezca por el Derecho de la Unión o de los Estados Miembros según la normativa especial que resulte de aplicación. Por ejemplo, la Ley 16/1985, de 25 de junio, reguladora del Patrimonio Histórico Español, entre otras. Esta exención, no exime para que un tratamiento sea lícito, que concurra alguna de las bases jurídicas previstas en el artículo 6.1. RGPD.

El tratamiento de datos lícitamente obtenidos para otra finalidad por la cual se recabaron, en atención al artículo 5.1 b), cuando se trate de investigación científica e histórica no se considerará incompatible con los fines iniciales y no precisará de una base jurídica distinta de la que permitió la obtención de los datos personales.

En cambio, si son datos obtenidos por primera vez, deberá concurrir alguna de las bases del artículo 6.1, entre las que se podría encontrar la letra e) con respecto de las investigaciones incluidas en los planes de investigación científica regulados por la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

Por lo tanto, habrá que valorar en el caso concreto si la investigación afecta o no a categorías especiales de datos, si los datos objeto de la misma ya se habían obtenido para otros fines o se obtienen por primera vez, si resulta de aplicación la Ley 14/2011 o si se establecen normas especiales en las leyes que regulen el tratamiento, los datos concretos o las fuentes de procedencia.

11. Publicación de la evaluación de los tramos de investigación del personal de las universidades

En este supuesto, el tratamiento se encuentra amparado en lo previsto en la letra e) del artículo 6.1 del RGPD, al ser la educación universitaria un servicio público que precisa, para garantizar la calidad como fin esencial de la política universitaria, contar con los profesionales mejor cualificados, tal y como se deduce de los artículos 31.1, 39.1 y 40.1 de la Ley Orgánica de Universidades.

12. Calificaciones obtenidas por los alumnos al amparo de lo previsto en la disposición adicional vigésimo primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

La publicación de las calificaciones universitarias tiene su base de legitimación en el art. 6.1.e) RGPD pero también puede encontrarse en el art. 6.1.f) RGPD porque como sostiene la AEPD: “aun no tratándose los procedimientos de evaluación de procedimientos de concurrencia competitiva, las calificaciones obtenidas van a tener incidencia […] en el otorgamiento de las matrículas de honor limitadas a un número de estudiantes, así como también en la concesión de premios extraordinarios, por lo que también podría apreciarse un interés legítimo de los alumnos del grupo en el conocimiento de las calificaciones de sus compañeros”.

La forma apropiada de publicar las calificaciones conforme a la normativa de

protección de datos ha sido desarrollada en la Universidad de Granada y puede consultarse en: “Publicación de calificaciones del estudiantado Universidad de Granada” .

13. Acceso a imágenes de cámaras de seguridad por incidente en un vehículo.

Las peticiones de terceros de acceso a determinadas imágenes grabadas por las cámaras de videovigilancia con el fin de entablar acciones judiciales y/o contractuales deben entenderse desde la óptica de solicitud de comunicaciones de datos o cesión de datos y no como ejercicio del derecho de acceso.

En cualquier caso, siempre y cuando la comunicación resulte necesaria para su presentación en juicio, se podría considerar la existencia de un interés legítimo conforme al artículo 6.1 f) del RGPD, en el que el derecho a la tutela judicial efectiva y de defensa de la persona prevalecería sobre el derecho a la protección de datos del afectado. La cesión o comunicación, habrá de limitarse al mínimo necesario o imprescindible para la finalidad pretendida en atención al principio de minimización.

En los supuestos en que, la cesión sea solicitada por las Fuerzas y Cuerpos de Seguridad del Estado, actuando como Policía Judicial, siempre que exista mandamiento judicial o requerimiento de la Fiscalía, la base de legitimación será el artículo 6.1 c) al tratarse de una obligación legal que exige un deber de colaboración con los Juzgados y Tribunales o con el Ministerio Fiscal según dispone el artículo 236 quáter de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y el artículo cuarto apartado cinco de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

No sería factible, sin embargo, autorizar la cesión de datos si tuviese por objeto o fin algo distinto de las finalidades para las que se recogieron los datos, contraviniendo la legislación de protección de datos.

14. Comunicación de los datos a las entidades aseguradoras

Quien sea solicitante, debería acreditar uno de los títulos habilitantes de los recogidos en el art. 6 RGPD, como podría ser el cumplimiento de una relación contractual o el cumplimiento de una obligación legal, conforme al artículo 6.1 apartados b) y c) RGPD, respectivamente.

15. Publicación listados con identificación de participantes en procedimientos de concurrencia competitiva

La publicación de listados con identificación de participantes en procedimientos de concurrencia competitiva se ampara en lo dispuesto en la letra c) del artículo 6.1.del RGPD, al venir impuesta por el artículo 45.1 de la Ley 39/2015, de 1 de octubre, de procedimiento Administrativo Común de las Administraciones Públicas.

Sin embargo, deberá ajustarse a las exigencias del principio de minimización, en particular si “el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos”. En este caso deberá limitarse la publicación a una mera indicación del contenido del acto, lugar donde los interesados deberán comparecer, el plazo indicado y el contenido integrado del mencionado acto, evitando en las referencias expresas al tipo de discapacidad o el grado.

Las indicaciones para la publicación de calificaciones universitarias son aplicables a estos supuestos para enmascarar apropiadamente el documento nacional de identidad, número de identidad extranjero, pasaporte o documento equivalente. Igualmente es aplicable a los centros electorales que publica la Universidad.

- Para consultar o descargar el informe completo pulse aquí.

La UGR coordina la elaboración de una Guía de Buenas Prácticas en Materia de Transparencia y Protección de Datos de la CRUE Universidades Españolas (Protección de Datos Personales - 25 de septiembre de 2019)

La publicación de la Ley 19/2013, de Transparencia,Acceso a la Información Pública y Buen Gobierno en diciembre de 2013; el Reglamento General de Protección de Datos, de plena aplicación desde mayo de 2018, así como la de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, el pasado mes de diciembre, hicieron necesario la posibilidad de contar con una Guía de buenas prácticas que recogiera las principales cuestiones recibidas en las Universidades sobre temas de transparencia y protección de datos.

A lo largo de 13 apartados, la Guía pretende **ofrecer a las universidades respuestas fundadas jurídicamente,** a tenor de la legislación vigente, de la jurisprudencia y de los criterios establecidos por los distintos órganos de control en materia de Transparencia y/o Protección de Datos. El texto se contempla como un **documento abierto** –sujeto a aportaciones, revisiones y modificaciones–, que podrá ser objeto de actualización y ampliación a través del **Grupo de Trabajo de Protección de Datos de Crue–Secretarías Generales.**

En definitiva, se trata de una herramienta viva que irá evolucionando según vayan progresando desde el punto de vista jurídico las diferentes materias que se contemplan como puedan ser los cambios normativos, las nuevas sentencias o las nuevas resoluciones de las agencias de control.

- Para consultar o descargar la guía pulse aquí.

Informe sobre publicación de calificaciones de asignaturas de Grado (Protección de Datos Personales - 30 de mayo de 2019)

La Agencia Española de Protección de Datos (AEPD) ha emitido un informe jurídico en relación con la publicación de las calificaciones de asignaturas impartidas en los estudios de Grado.

La AEPD concluye que **es lícita la publicación de las notas obtenidas en los estudios de Grado** de conformidad con los dispuesto en el Reglamento General de Protección de Datos (RGPD), al estar amparada en la existencia de un **interés público (art. 6.1.e RGPD)**, al que debe sumarse un **interés legítimo de los alumnos del grupo** en el conocimiento de las calificaciones de sus compañeros **(art. 6.1.f RGPD).**

En todo caso deberán respetarse los **principios recogidos en el artículo 5 del RGPD**, especialmente los de limitación de la finalidad, minimización de datos, limitación del plazo de conservación, integridad y confidencialidad, realizando la publicación de modo que suponga la menor injerencia en los derechos y libertades de los interesados, lo que **excluye la posibilidad de un conocimiento generalizado** de las calificaciones o su publicación en internet. De ahí que se considere preferente proceder a dicha publicación a través de una **intranet o aula virtual** en la que estuviera **limitado el acceso a los profesores y compañeros del grupo**. **En el caso de que no fuera posible**, podrá realizarse en los **tablones de anuncios del centro**, siempre que **no se encuentren en las zonas comunes** de los centros, se garantice el acceso restringido a dichas personas y se adopten las medidas necesarias para evitar su público conocimiento por quienes carecen de interés.

En cuanto a los **datos a publicar**, atendiendo al principio de minimización, deberán limitarse al nombre y apellidos del alumno y la calificación obtenida. Solo en el caso de que hubiera alumnos con los mismos nombres y apellidos, deberá publicarse para ellos el número del DNI, aplicando lo previsto en el apartado 1 párrafo primero de la disposición adicional séptima de la LOPDGDD.

Finalmente, en cuanto al **tiempo en el que deberá mantenerse dicha publicación**, los datos deberán ser mantenidos durante no más tiempo del necesario para los fines del tratamiento de los datos personales (artículo 5.1.e. del RGPD). Por tanto, en el caso de las calificaciones provisionales, mientras transcurre el plazo para presentar reclamaciones, y las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.

- Para consultar el informe completo pulse aquí.

Listado de tratamientos en los que es obligatorio realizar una evaluación de impacto (Protección de Datos Personales - 8 de mayo de 2019)

El Reglamento General de Protección de Datos (RGPD) establece en su artículo 35.1 que, en aquellos casos en los que sea probable que los tratamientos entrañen un alto riesgo para los derechos y libertades de las personas físicas, incumbe al responsable del tratamiento realizar una evaluación de impacto (EIPD) relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad del riesgo. Por otro lado, el apartado 4 de ese mismo artículo prevé que cada autoridad de control establezca y publique una lista de los tipos de operaciones de tratamiento que requieran de una evaluación de impacto.

La Agencia Española de Protección de Datos (AEPD) ha publicado el **listado de tratamientos de datos personales en los que es obligatoria la realización de una evaluación de impacto**. Esta lista tiene, por tanto, la finalidad de ofrecer seguridad a los responsables respecto a cuáles son los tratamientos en que siempre se considerará que es probable que exista un alto riesgo. También de acuerdo con lo previsto por el RGPD, la lista ha sido comunicada al Comité Europeo de Protección de Datos, que ha emitido un dictamen favorable sobre ella, siguiendo los criterios establecidos en la valoración de todas las listas remitidas por las autoridades nacionales.

La Agencia Española de Protección de Datos (AEPD) **advierte que** será necesario realizar una EIPD en la mayoría de los casos en los que en los que el tratamiento cumpla con dos o más criterios de la lista, entre los que se encuentran la realización

de perfilado; observación, geolocalización o control de forma sistemática y exhaustiva; el uso de datos biométricos para identificar de forma unívoca a una persona; datos que permitan determinar la solvencia patrimonial o procesamiento de identificadores únicos que permitan identificar usuarios de servicios de la sociedad de la información como pueden ser los servicios web, televisión interactiva o aplicaciones móviles, entre otros tratamientos. Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe y mayor la certeza de la necesidad de realizar una evaluación de impacto.

- Puede consultar el listado aquí.

Orientación para la aplicación provisional de la Disposición Adicional 7.ª de la LOPDGDD (Protección de Datos Personales - 8 de mayo de 2019)

La Agencia Española de Protección de Datos (AEPD) ha publicado unas orientaciones para promover la **protección de los datos personales de los ciudadanos cuando las Administraciones Públicas realizan publicaciones de actos administrativos.** El documento se publica en coordinación con la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

La Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y garantía de los derechos digitales (LOPDGDD) incluye en el apartado 1º de su Disposición Adicional 7ª cómo debe identificarse a los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

El criterio, provisional hasta que los órganos de gobierno y las administraciones públicas competentes aprueben disposiciones para la aplicación de la Disposición, pretende evitar que la adopción de otras fórmulas pueda dar lugar a la publicación de cifras numéricas de los documentos identificativos de las personas en posiciones distintas, posibilitando la recomposición íntegra de dichos documentos. Para ello, se ha seleccionado aleatoriamente un grupo de cuatro cifras numéricas, que deberían ser las mismas en todas las publicaciones.

- Puede acceder aquí al contenido del documento con las orientaciones.