10ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

# Preguntas de los asistentes

www.aepd.es

@AEPD_es #10SesiónAEPD

¿Cómo debería configurarse el consentimiento explícito para el uso de tecnologías biométricas de reconocimiento facial en la entrada de establecimientos en el caso de que no aplique ninguna de las excepciones reguladas en el artículo 9?

- Conforme al considerando 51 del RGPD el tratamiento del rostro con software de reconocimiento facial se encuentra dentro de los datos biométricos.
- Para resolver la cuestión habrán de tenerse especialmente en cuenta los principios de minimización y de licitud del tratamiento (en este caso de categorías especiales de datos).
- En el ámbito laboral el uso de estas tecnologías podría considerarse una medida de control por el empresario, admitida por el artículo 20 ET siempre y cuando sea proporcional, lo que exigiría tener en cuenta la naturaleza de la actividad y de las instalaciones para cuyo acceso se requiriese el reconocimiento facial.
- En los restantes supuestos no existiría una habilitación similar, si bien podría ser posible el tratamiento cuando se tratase de preservar la seguridad de determinadas instalaciones. Como las estratégicas, así como en determinados supuestos amparados por la Directiva 2016/680

Actualmente la mayoría de los aparatos fichadores de las empresas son por huella dactilar. Sería un dato biométrico dirigido a identificar de manera unívoca a cada persona física (la totalidad de la muestra). ¿Debo pedir consentimiento expreso y libre a cada trabajador? ¿Si un trabajador no me lo da, tendré que proporcionarle otro método de fichaje?

- El tratamiento de la huella digital para el control de acceso por los trabajadores podría considerarse una medida de control amparada en el artículo 20 del Estatuto de los Trabajadores, por lo que no exigiría consentimiento del empleado.
- No obstante, para implantar esta medida debería aplicarse el principio de minimización; es decir, debería limitarse a los supuestos en que se considere realmente necesaria para que el control sea eficaz.
- La AEP ha señalado en diversos informes que podrían existir buenas prácticas que permitieran el control a través de la huella digital sin que el sistema tuviera que almacenar el dato biométrico (por ejemplo por su incorporación a una tarjeta inteligente que se contrastase con la huella y se mantuviera siempre en poder del trabajador).

¿Se deben considerar los proveedores de servicios de internet (sin servicios adicionales a la conexión a internet) como encargados de tratamiento si se usan sus infraestructuras para el envío de datos? En caso afirmativo ¿debería considerarse una transferencia internacional por tener parte de la infraestructura fuera de la unión europea?

- Si se está haciendo referencia a un operador de acceso a Internet en los términos definidos por la Ley General de Telecomunicaciones y no presta ningún servicio adicional en que pueda tener la condición de encargado, no nos encontraríamos ante un encargado del tratamiento, dado que el uso de la red pública de comunicaciones no implicaría un tratamiento por cuenta de los emisores y receptores de los datos que pudiera incluir una comunicación

¿Como se aplica el principio de interés legítimo para dar cumplimiento a derechos derivados de la gestión de cobro de deudas vencidas, líquidas y exigibles. así como a las obligaciones legales como la prevención del blanqueo de capitales y la financiación del terrorismo?

¿Todos los sujetos obligados en prevención del Blanqueo de Capitales precisan tener un DPD independientemente del volumen de clientes?

- En el supuesto de contratación de una entidad para la gestión de cobros la AN viene sosteniendo que se trataría de un encargado del tratamiento, por lo que no será necesario amparar la transmisión en el interés legítimo, sin que exista un contrato con los requisitos del artículo 28 del RGPD.
- El cumplimiento de las obligaciones legales en prevención del blanqueo de capitales se encontraría amparado en el artículo 6.1 c) del RGPD y no en el 6.1 f). Igualmente, la creación de sistemas comunes de información podría ampararse en el artículo 6.1 e), dada la naturaleza de estas obligaciones, siempre que existan garantías adecuadas.
- En cuanto a la exigibilidad de un DPD, como regla general sólo se considera que están incluidos en los supuestos del RGPD por los tratamientos específicos relacionados con prevención del blanqueo los gestores de los ficheros comunes previstos en el artículo 33 de la Ley 10/2010. No obstante, muchos sujetos obligados deberían contar con un DPD como consecuencia de la actividad que desarrollan en general.

## ¿Qué ocurrirá hasta que se apruebe la nueva LOPD con el tratamiento de datos de los autónomos y los datos de contacto de las personas que prestan sus servicios en las empresas y autónomos (teléfono, email, etc.)?

- Como punto de partida, no cabe considerar que estos datos no sean datos de carácter personal, dado que se refieren a personas físicas identificadas.
- Aun cuando aún no se haya aprobado la nueva Ley, siempre que el tratamiento se realice en las condiciones que la misma indican, podría considerarse que existe una presunción a favor del interés legítimo del responsable y el tratamiento podría ampararse en el artículo 6.1 f) del RGPD.

Actualmente la mayoría de los aparatos fichadores de las empresas son por huella dactilar. Sería un dato biométrico dirigido a identificar de manera unívoca a cada persona física (la totalidad de la muestra). Debo pedir consentimiento expreso y libre a cada trabajador?

- Si un trabajador no me lo da, tendré que proporcionarle otro método de fichaje?
- El tratamiento de la huella digital para el control de acceso por los trabajadores podría considerarse una medida de control amparada en el artículo 20 del Estatuto de los Trabajadores, por lo que no exigiría consentimiento del empleado.
- No obstante, para implantar esta medida debería aplicarse el principio de minimización; es decir, debería limitarse a los supuestos en que se considere realmente necesaria para que el control sea eficaz.
- La AEP ha señalado en diversos informes que podrían existir buenas prácticas que permitieran el control a través de la huella digital sin que el sistema tuviera que almacenar el dato biométrico (por ejemplo por su incorporación a una tarjeta inteligente que se contrastase con la huella y se mantuviera siempre en poder del trabajador).

¿Cabe apreciar el interés legítimo como base legitimadora e las transmisiones de datos entre las entidades de un mismo grupo que tienen la misma matriz y consolidan cuentas? ¿Se puede hablar de un interés legítimo de grupo?

- El artículo 6.1 f) del RGPD indica que el interés legítimo debe concurrir en el responsable o en el tercero al que se comunican los datos. Por este motivo, en los grupos, el interés debería apreciarse de cada responsable y no del Grupo, sin perjuicio de los supuestos de corresponsabilidad.
- No obstante, es cierto que en los supuestos de grupos la trasmisión intra grupo puede en ocasiones estar fundada en el interés legítimo de todas las empresas del Grupo, lo que deberá ser especialmente tenido en cuenta en atención a las circunstancias de cada caso. Además, existen distintas normas que imponen la obligación de comunicación intra grupo y ampararían esa transmisión en el artículo 6.1 c) del RGPD, especialmente cuando se habla de grupos consolidados.

## ¿Qué se entiende como fuentes de acceso público?

- A día de hoy, con el RGPD en vigor, no puede hablarse de un concepto legal de «fuentes accesibles al público» como el que existía en la LOPD ni de que el hecho de que los datos aparezcan en este tipo de fuentes legitime sin más el tratamiento.
- El RGPD sólo habla de fuentes de acceso público al regular el derecho a la información si los datos no se han recogido del interesado.
- El hecho de que un dato sea accesible por cualquiera puede ser tenido en cuenta a la hora de realizar la ponderación del artículo 6.1.f) (como decía la STJUE Asnef), pero no implica necesariamente que el tratamiento vaya a ser lícito, por cuanto se deben respetar los restantes principios del RGPD

¿Cómo ha de interpretarse la exclusión del deber de información cuando los datos no son obtenidos del titular y existe una obligación de secreto profesional regulada prevista en el artículo 14.5.d) del RGPD?

- Esta excepción ya estaba recogida en el RLOPD y se refiere a los supuestos en que una norma de derecho de la Unión o de derecho interno obligan a quien trata datos a no advertir al interesado de que se está llevando a cabo este tratamiento. Así sucede, por ejemplo, en materia de prevención del blanqueo de capitales, en que existe la obligación legal expresa de no revelar a una persona que está siendo sometida a examen especial.
- El artículo añade igualmente los deberes de secreto profesional establecidos para determinadas profesiones y que podrían perjudicar a terceros. Así por ejemplo, como viene diciendo la AEPD desde el año 2000, no procede que los abogados informen a la contraparte de su cliente acerca del tratamiento de sus datos, porque ello contravendría el secreto profesional y el derecho a la defensa del que es titular el cliente

Para tratar a nivel profesional datos personales de carácter penal de mayores de edad en un despacho de abogados ¿es necesario algo más que el consentimiento expreso prestado y firmado expresamente por el cliente al contratar el servicio?

- El hecho de que una persona solicite la asistencia de un despacho de abogados, máxime en el marco de un proceso penal, constituye una clara acción afirmativa que legitima el tratamiento de los datos por el abogado.
- En todo caso, dicho tratamiento es necesario para garantizar el derecho a la asistencia letrada establecido, como parte de la tutela judicial efectiva, por el artículo 24.2 de la Constitución

## Deber de informar a los empleados. Una primera información en el contrato y remisión a una segunda capa no pública. ¿Se deben detallar los encargados del tratamiento o se pueden indicar categorías generales tipo gestoría?

En cuanto a la información por capas se puede consultar la Guía para el cumplimiento del deber de informar (www.aepd.es)

En todo caso en la primera capa debe incluirse la siguiente información:

- Identidad del responsable del tratamiento o su representante
- Finalidad del tratamiento
- Modo de ejercicio de los derechos

Las comunicaciones de datos a los encargados de tratamiento no se consideran cesiones de datos y no es necesario informar de ellas a los interesados

Las empresas que no hayan pedido el consentimiento de sus clientes antes del 25 de mayo ¿podrían solicitarlo con posterioridad?

Habría que realizar un análisis del tratamiento de los datos y de sus fines para determinar cuál es su base jurídica

Si se basará en el consentimiento y éste se hubiera obtenido previamente de manera no tácita, no sería necesario recabarlo nuevamente

En todo caso, antes de realizar un tratamiento de datos se debe contar con la correspondiente legitimación (art. 6.1 RGPD)

Las encuestas de satisfacción y el ofrecimiento de productos y servicios a clientes de la misma empresa que le vendió el producto o servicio ¿pueden considerase un tratamiento basado en el interés legítimo, conforme al considerando 47 del RGPD?

Además de observar la LSSI, si ambos supuestos son consecuencia de una relación previa de carácter contractual y se refirieren a productos y servicios objeto de dicho contrato cabría amparar el tratamiento de datos en el interés legítimo, previa su correspondiente ponderación con los derechos y libertades de los interesados que deberá quedar documentada

## ¿En cuánto está estimado el tiempo de respuesta a las peticiones de normas corporativas vinculantes (BCR)?

En primer lugar, dependerá de la duración de las aproximaciones informales que se tengan con la autoridad de control

El WP 263 rev.01 del Grupo del 29 establece el procedimiento de cooperación para la aprobación de BCR en el marco del RGPD

Por último, el PLOPD recoge un plazo máximo de 1 año, que s suspenderá durante la tramitación del procedimiento de cohesión en el CEPD

Queremos recabar los datos y que la firma sea la única acción afirmativa. El fin comercial incluye: evaluar y predecir las preferencias del cliente y ceder los datos con fines comerciales a la matriz ¿con la simple firma es suficiente dado que la elaboración de perfiles y la cesión de los datos es para la misma finalidad comercial? O por el contrario ¿debemos poner dos casillas por cada subfinalidad comercial?

- Predecir las preferencias del cliente o elaborar perfiles del mismo es un tratamiento que debe tener su base jurídica propia conforme al RGPD. Es un tratamiento distinto al realizado con fines publicitarios que debe tener su propia base jurídica.
- La cesión de datos con fines comerciales a la matriz debe estar separada ya que supone una comunicación de datos a terceros y no se indica con precisión qué finalidades comerciales (¿de productos similares, de productos distintos, de productos de terceros..?).
- En todo caso debe tenerse en cuenta el sistema de garantías específico de la Ley General de Telecomunicaciones y de la LSSI.

- Si la firma es en el marco de un contrato en el que se incluyen cláusulas que no tienen relación con el objeto del mismo, la información y la decisión debe realizarse separadamente.

¿Será suficiente con habilitar un check-out para clientes en el marco de la mercadotecnia directa cuando esta se realice con perfilado hecho exclusivamente con información obtenida de fuentes internas de la compañía?

- Predecir las preferencias del cliente o elaborar perfiles del mismo es un tratamiento que debe tener su base jurídica propia conforme al RGPD. Es un tratamiento distinto al realizado con fines publicitarios que debe tener su propia base jurídica, **aunque la información se haya obtenido de fuentes internas de la compañía**.

Buenos días, me gustaría saber si se puede enviar publicidad si hay una casilla desmarcada () texto no quiero recibir publicidad. Si después se pulsa un acepto la política de privacidad. Muchas gracias. Un saludo.

- No.

## POSIBILIDAD DE SUSTITUIR LA EVALUACIÓN DE IMPACTO DE TRATAMIENTOS PREVIOS QUE SEGUIRÁN APLICÁNDOSE DESPUÉS DE LA ENTRADA EN VIGOR DEL RGPD POR LAS ÁREAS DE MEJORA DETECTADAS EN INFORMES DE AUDITORÍA DE PROTECCIÓN DE DATOS, ASÍ COMO TAMBIÉN INFORMACIÓN QUE DERIVE DEL REGISTRO DE INCIDENCIAS PREEXISTENTE

Las evaluaciones de impacto tienen un objetivo distinto al de las auditorías, las auditorías se orientan a evaluar los resultados de las medidas y su puesta en marcha. La evaluación de impacto determina los riesgos de un tratamiento con carácter previo a su puesta en marcha.

# NECESIDAD -O NO- DE REALIZAR EVALUACIONES DE IMPACTO EN LOS TRATAMIENTOS DE LAS ACTIVIDADES DE UNA UNIVERSIDAD PÚBLICA -SECTOR PÚBLICO-

Artículo 35:

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

# LAS AUDITORIAS BIENALES ¿SIGUEN SIENDO OBLIGATORIAS?

Las auditorías forman parte de cualquier metodología de análisis de riesgos, ahora es el responsable quien decide sobre la periodicidad de las mismas. No son preceptivas pero si necesarias.

VER EJEMPLOS DE

1.- CÓMO SE VALORA LA GRAN ESCALA EN EL TRATAMIENTO,

2.- SI HAY O NO OBSERVACIÓN HABITUAL Y SISTEMÁTICA DE INTERESADOS,

3.- CÓMO VALORAMOS SI SE REALIZA UN SEGUIMIENTO FRECUENTE Y REPETITIVO

4.- QUÉ SE CONSIDERA UN MÉTODO DE ORGANIZACIÓN, CLASIFICACIÓN U ORDENACIÓN DE SUS DATOS

- **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (4 de abril de 2017)**

**- Concepto de fichero en el artículo 4.6 del RGPD**

# ANÁLISIS DE RIESGO Y EVALUACIÓN DE IMPACTO ¿CÓMO DE FORMA EFICIENTE?

- METODOLOGÍA DE ANÁLISIS DE RIESGO:
  - Identificar amenazas y riesgos
  - Evaluar riesgos
  - Tratar riesgos
  - Monitorizar

EL ARTÍCULO 34 DE EU-GDPR ESTABLECE QUE, SI LOS DATOS ESTÁN CIFRADOS, ENCRIPTADOS, NO ES NECESARIO NOTIFICAR A LOS AFECTADOS EN CASO DE FUGA DE LOS MISMOS.

¿HA ELABORADO LA AEPD UN CATÁLOGO DE SOLUCIONES DE ENCRIPTACIÓN LO SUFICIENTEMENTE ROBUSTAS COMO PARA ASEGURAR QUE LOS DATOS NO SON LEGIBLES POR TERCEROS?

Corresponde al responsable y encargado del tratamiento aplicar las medidas técnicas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en función del estado de la técnica (Art. 32).

El responsable y el encargado deben decidir sobre los algoritmos de cifrado que consideren necesarios en cada caso atendiendo a los estándares del mercado.

## Requisitos para trabajar como delegado de protección de datos, certificación necesaria, cómo acreditarse, entidades de formación homologadas, etc.

Los que determina el RGPD en su artículo 37.5:

*"El delegado de protección de datos 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 las funciones indicadas en el artículo 39."*

Por lo tanto, en ningún caso la certificación se convierte en un requisito. El DPD podrá optar por certificarse para ofrecer a responsables y encargados un valor añadido a sus servicios como DPD, la certificación es un elemento de confianza para el mercado de los profesionales de la privacidad y no un requisito.

La certificación del DPD tendrá lugar por parte de las entidades de certificación que hayan sido acreditadas por ENAC, corresponde a estas entidades de certificación comprobar los prerrequisitos de experiencia y formación de los candidatos y, por su parte, los candidatos deben acreditar ante las entidades de certificación dichos requisitos.

¿Se va a publicar una guía sobre amenazas y riesgos técnicos que impacten en los datos personales de cara a la realización y/o análisis de riegos y evaluaciones de impacto o a una ampliación de las actuales guías de evaluación de impacto y análisis de riesgos que determinen estos aspectos y amenazas de seguridad tecnológica?

Existen en el mercado estándares o catálogos de riesgos y salvaguardas aplicables para llevar a cabo la evaluación de riesgos de seguridad de la información (por ejemplo ENS, ISO2700). Sin perjuicio de que en el futuro puedan existir en el mercado otro tipo de catálogos de riesgos para los derechos y libertades de las personas que pudieran deducirse de los tratamientos de datos personales, el análisis necesario para determinar los riesgos y salvaguardas en cada caso siempre corresponderá al propio responsable.

El establecimiento de un marco de riesgos preceptivo para la generalidad de los tratamientos no sería posible y su posible existencia sería meramente como modelo orientativo y de mínimos. Corresponderá siempre particularizar los riesgos para cada caso o tratamiento específico.

Recientemente las grandes plataformas proveedoras de servicios cloud como Amazon, Google, etc. han obtenido su certificación para el esquema ENS en su nivel alto, qué otras consideraciones deberíamos valorar respecto a la privacidad de los datos además de revisar las cláusulas de los pliegos y establecer un contrato tipo de servicios basado en el cumplimiento del RGPD.

En primer lugar hay que tener en cuenta que la certificación en el marco del ENS es una manera en la que responsables y encargados pueden demostrar "accountability" o proactividad en especial en lo referido a las medidas de seguridad técnicas y organizativas.

Los contratos de servicios de cloud pueden incluir el resto de detalles necesarios para articular la prestación de servicios con las garantías técnicas y organizativas que pudieran ser necesarias para garantizar los derechos y libertades de los ciudadanos. Por ejemplo, se pueden articular procedimientos de notificación de brechas de seguridad, procedimientos para atender los derechos de los interesados o definir con claridad la relación entre el DPD del proveedor del servicio de cloud y el DPD del cliente.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS


www.aepd.es

@AEPD_es #10SesiónAEPD

10ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS