PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 07/20

EL RGPD UE 2016/679 EN APLICACIÓN

La protección de datos desde el diseño y por defecto

El responsable del tratamiento, en virtud de su responsabilidad proactiva, debe definir anticipadamente y de forma preventiva el tratamiento de los datos personales. En las primeras fases del diseño de las operaciones del tratamiento, se tendrán que aplicar las medidas técnicas y organizativas que garanticen la protección de los datos personales desde el primer momento. **Esto es lo que se denomina protección de datos desde el diseño.**

¿Qué significa entonces, el concepto por defecto? El responsable en este caso, debe garantizar que los datos se traten con la mayor protección de la intimidad posible. Es decir, solamente se tratarán los datos necesarios para la finalidad del tratamiento, el plazo de conservación será el mínimo imprescindible y la accesibilidad a esos datos será limitada.

¿Y cómo puede el responsable aplicar estos principios y demostrar además su cumplimiento? Lo puede hacer mediante la realización de la Evaluación de Impacto de protección de datos regulada en el art.35 del RGPD. En determinados supuestos la evaluación de impacto resultará obligatoria, en particular, cuando se vayan a utilizar nuevas tecnologías que entrañen un alto riesgo para los derechos y libertades de los interesados.

Contenido

IMPORTANTE

En este listado publicado por la AEPD se recogen los tratamientos que requieren una evaluación de impacto.

SANCIONES DE LA AEPD

Un hotel sancionado por ubicar una cámara de videovigilancia grabando parte de la vía pública

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00369-2019.pdf instruido por la AEPD, se sanciona a CASA GRACIO OPERATION, SLU (el reclamado), por la colocación de cámaras de videovigilancia grabando parte de la vía pública.

En este caso, el reclamante, una comunidad de propietarios, alegaba que las cámaras de videovigilancia de dicho hotel recogían imágenes de la vía pública, así como parte de la puerta de entrada a su comunidad. Para ello, en su escrito, presentó fotografías de la ausencia de carteles y de la ubicación de los dispositivos de videovigilancia y sus modelos.

La AEPD admite a trámite la reclamación e inicia un proceso de investigación. La reclamada presentó pruebas alegando que las cámaras cumplían con la normativa de protección de datos. Después de realizar las oportunas comprobaciones, la AEPD estima que no es así, ya que las cámaras instaladas tipo Domo poseen máscaras de privacidad que no son las adecuadas para la protección de los datos personales, puesto que recogen un perímetro mayor del permitido.

Se vulnera uno de los principios básicos del RGPD que es el de la minimización de datos, ya que las imágenes que captan estas cámaras son excesivas para cumplir con la finalidad de videovigilancia del Hotel. Se sanciona con 10.000 euros. El reclamado acepta su responsabilidad por lo que la cantidad al final fue menor.

La AEPD puede ordenar al responsable o encargado determinadas actuaciones, su incumplimiento es objeto de sanción.

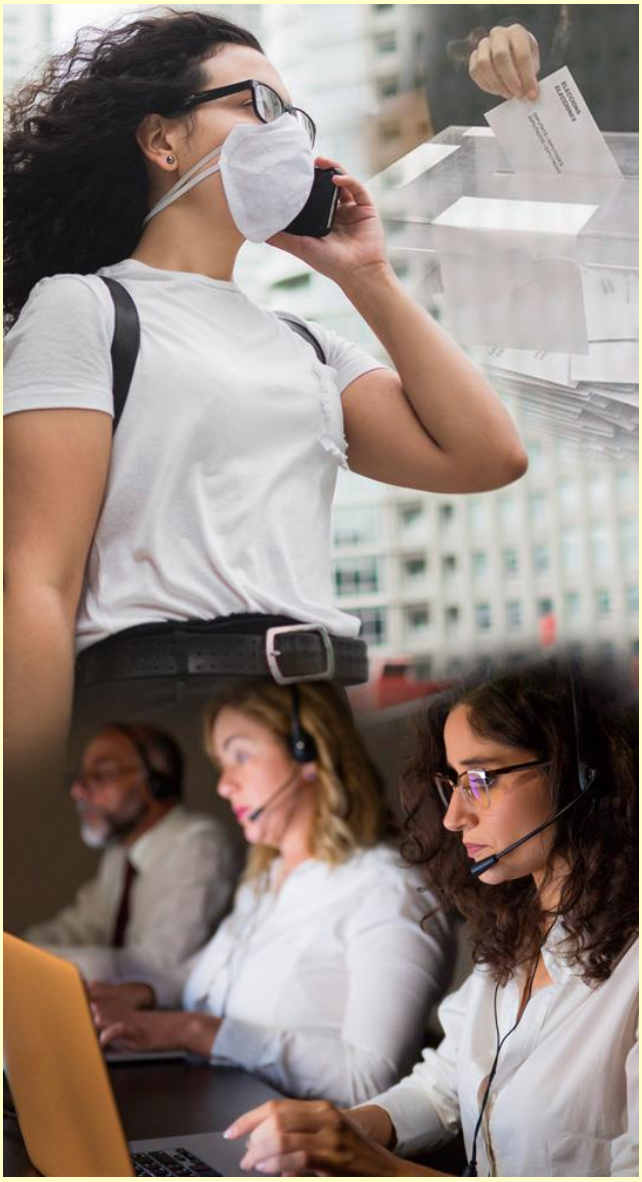
IMPORTANTE

Estaría permitido captar mínimamente parte de la vía pública, solamente, en el caso de no existir otra alternativa de instalación de las cámaras.

LA AEPD ACLARA

¿Es posible ceder datos telefónicos al CIS para realizar encuestas telefónicas?

La consulta es planteada a la AEPD https://www.aepd.es/es/documento/2020-0049.pdf por el CIS (Centro de Investigaciones Sociológicas) ante la necesidad de acceder a los listados de teléfono para la realización de las encuestas pre electorales vascas y gallegas.



La AEPD resuelve si esta cesión es legítima y si cumple con las garantías para su realización conforme a la normativa de protección de datos.

El CIS justifica que debido a la situación especial derivada por la COVID-19 y las restricciones del estado de alarma, las encuestas no se pueden realizar mediante visita personal, tal y como marca la normativa que regula la función estadística. por otro lado, la utilización del correo ordinario para este tipo de estudios no se ajustaría a los objetivos de la encuesta. Por eso entiende, que la única posibilidad es realizar mediante llamada telefónica. En este sentido, la AEPD señala en su informe, que la justificación planteada por el CIS es adecuada.

Además, la AEPD indica que se deben aplicar los principios del RGPD, como es el de minimización de los datos. Solamente se facilitará el número de teléfono y la provincia, pero no su titular; se dará acceso a un porcentaje que se ajuste a la muestra y se podrán conservar el tiempo necesario para hacer el trabajo de campo, hasta un máximo de 30 días. Se tendrán en cuenta, por otro lado, las garantías propias de la función estadística.

IMPORTANTE

No se cederán los datos telefónicos de aquellas personas que hayan ejercitado su derecho a no figurar en las guías accesibles al público.

ACTUALIDAD LOPD

La AEPD publica un listado con los equívocos más comunes con el uso de la biometría y protección de datos

Fuente: AEPD

(Madrid, 23 de junio de 2020). La Agencia Española de Protección de Datos (AEPD) ha publicado una nota técnica que incluye catorce equívocos relacionados con el uso de la biometría y cómo afectan a la protección de datos. El documento, dirigido a responsables, encargados y Delegados de Protección de Datos, entre otros, tiene como objetivo ofrecer información acerca de las confusiones e imprecisiones más comunes que suelen asociarse al empleo de esta tecnología, de forma que estos colectivos **puedan comprender las implicaciones de un tipo de tratamiento tan complejo**.

La nota técnica ha sido desarrollada junto al Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés) en el marco de la colaboración que mantiene la AEPD en el ámbito tecnológico con diversas instituciones nacionales e internacionales. La colaboración con el EDPS se materializó por primera vez en el desarrollo de la nota técnica Introducción al hash como técnica de seudonimización de datos personales.

El Reglamento General de Protección de Datos (RGPD) define en su artículo 4 los datos biométricos como aquellos "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". Asimismo, cuando los datos biométricos se usan como medio de identificación, el RGPD establece en su artículo 9 que se trata de categorías especiales de datos y prohíbe expresamente su tratamiento dirigido a identificar de manera unívoca a una persona física.

Entre los equívocos más comunes relacionados con la biometría se encuentra la afirmación de que **los sistemas de identificación y autenticación biométrica son más seguros para los usuarios**. En este sentido, la Agencia advierte de que el acceso no autorizado a datos biométricos en un sistema permitiría o facilitaría el acceso en el resto de los sistemas que utilicen dichos datos biométricos. Esto tendría el mismo efecto que usar la misma contraseña en muchos sistemas distintos y, a diferencia de los sistemas basados en contraseñas, una vez que la información biométrica ha sido comprometida, esta no se puede cancelar. También alerta de que la información biométrica se almacena cada vez en más entidades y dispositivos, lo que aumenta exponencialmente la probabilidad de una brecha de seguridad de información biométrica.

Puede ver más información en el siguiente enlace

Nota técnica 14 equívocos con relación a la identificación y autenticación biométrica

EL PROFESIONAL RESPONDE

¿Puedo conservar un currículum en el que se incluye el dato sobre el estado de inmunidad frente a la COVID-19?

Actualmente, se están viviendo situaciones paradójicas en materia de protección de datos debido a la pandemia que estamos sufriendo por la COVID-19.

Recientemente, la AEPD se ha pronunciado en un comunicado a cerca del tratamiento de datos de salud incluidos en el currículum vitae de los solicitantes a un empleo.

El dato de salud en cuestión, es el referido al estado de inmunidad frente a la enfermedad.

Primero, el responsable de una entidad no puede solicitar este dato para incluirlo dentro del proceso de selección como un requisito, ya que, se estaría llevando a cabo un tratamiento de datos de categorías especiales sin una finalidad legitima. Por otro lado, la legitimación del tratamiento es ilícita. Este supuesto no puede fundamentarse en el consentimiento del candidato, no sería válido, puesto que en esta situación no se daría libremente. Tampoco se podría alegar una necesidad para la celebración del contrato y aplicar las medidas de prevención. El responsable debe mantener la seguridad en su centro de trabajo, respecto de sus trabajadores y el futuro candidato aún no lo es.

En segundo lugar, cuando un responsable reciba un currículum vitae incluyendo este dato sobre el estado de inmunidad del candidato debería eliminarlo de su base de datos.

IMPORTANTE

Pedir información sobre el estado de inmunidad frente a la COVID-19 va más allá de las obligaciones impuestas al empresario en la legislación laboral.