26/11/2023

La AEPD publica una guía sobre la utilización de datos biométricos para el control de presencia y acceso

- El documento fija los criterios de uso de esa tecnología tanto con fines laborales como no laborales
- La utilización de datos biométricos supone un tratamiento de categorías especiales de datos de alto riesgo
- El Reglamento General de Protección de Datos impone límites estrictos para el tratamiento de categorías especiales de datos, y la superación del análisis de idoneidad, necesidad y proporcionalidad

La Agencia Española de Protección de Datos (AEPD) ha publicado la Guía Tratamientos de control de presencia mediante sistemas biométricos, un documento que fija los criterios para la **utilización de la biometría** para el control de acceso, tanto con fines laborales como no laborales, estableciendo las medidas que tenerse en cuenta para que un tratamiento de datos personales que utilice esa tecnología cumpla con el Reglamento General de Protección de Datos (RGPD) entre otras normativas.

Los sistemas biométricos y el tratamiento de los datos que se pueden obtener a partir de ellos están evolucionando muy rápidamente. Los nuevos sistemas aumentan el detalle de la información recogida e incluso permiten la posibilidad de recoger información sin la cooperación de la persona, que en ocasiones ni siquiera es consciente de ello. A ello se suma el desarrollo de la inteligencia artificial, que puede utilizarse para inferir información adicional sobre las personas.

La Agencia considera el tratamiento de datos biométricos, **tanto para identificación como para autenticación**, como un tratamiento de **alto riesgo** que incluye **categorías especiales de datos**. Tal y como establece el RGPD, para poder tratar esas categorías es necesario que exista una circunstancia que levante la prohibición de su tratamiento y, además, una condición que lo legitime.

En el caso de registro de jornada y control de acceso **con fines laborales**, si el levantamiento de la prohibición se basa en el artículo 9.2.b) del RGPD, el responsable debe contar con una norma con rango de ley que autorice específicamente utilizar datos biométricos para dicha finalidad. La Agencia especifica que, en el marco de estos tratamientos, el consentimiento no puede levantar la prohibición o ser una base para determinar la licitud de este, al existir un desequilibrio entre la persona a la que se somete al tratamiento y quien lo está llevando a cabo.

En el caso del control de accesos **fuera del ámbito laboral**, el consentimiento tampoco podrá ser una circunstancia que levante la prohibición, al ser un tratamiento de alto riesgo, y no superar el requisito de necesidad (artículo 35.7.b).

La Guía también establece restricciones en los tratamientos biométricos realizados para el control de presencia cuando se toman **decisiones automatizadas sin intervención humana** que tengan efectos jurídicos sobre la persona o le afecten significativamente de modo similar.

En todo caso, la Guía precisa que, en caso de pretender captar datos biométricos, **de forma previa al inicio del tratamiento**, será obligatoria la realización de una Evaluación de Impacto para la Protección de Datos en la que, entre otros aspectos, se acredite la superación del triple análisis de idoneidad, necesidad y proporcionalidad del tratamiento.

Por último, la Agencia también añade un **listado de medidas** que deben llevarse a cabo si se superan todos los requisitos de

cumplimiento de los principios del RGPD:

– Informar a las personas sobre el tratamiento biométrico y los riesgos elevados asociados al mismo.
Implementar en el sistema biométrico la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física.
– Implementar medios técnicos para asegurarse la imposibilidad de utilizar las plantillas para cualquier otro propósito.
– Utilizar cifrado para proteger la confidencialidad, disponibilidad e integridad de la plantilla biométrica.
Utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.
– Suprimir los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento.
– Implementar la protección de datos desde el diseño.
Aplicar la minimización de los datos recogidos, con una evaluación objetiva de que no hay tratamiento de categorías especiales de datos.

Fuente: AEPD

LINK DE LA NOTICIA