RSM Alert

Diciembre de 2023

AEPD REDEFINE CRITERIOS: PROHIBIDO FICHAR CON HUELLA DACTILAR O RECONOCIMIENTO FACIAL, CAMBIO CRUCIAL EN CONTROL BIOMÉTRICO

PUNTOS CLAVE

- La Agencia Española de Protección de Datos (AEPD) prohíbe el uso de huella dactilar y reconocimiento facial para el control de acceso y presencia.
- Estos cambios entran en vigor con efecto inmediato, en respuesta a las directrices de la Unión Europea.

¿A QUIÉN AFECTA?

Afecta a empresas que utilizan sistemas biométricos para el control de presencia, tanto laboral como no laboral.

La nueva normativa impacta directamente en el tratamiento de datos biométricos, considerándolo de alto riesgo.

RECOMENDACIONES

- Revisar y ajustar los sistemas biométricos de control.
- Realizar una evaluación de impacto para la Protección de Datos.
- Informar a empleados/clientes sobre cambios y riesgos.

Alinearse con las nuevas restricciones de la AEPD sobre el uso de datos biométricos es crucial para evitar multas conforme al RGPD. Se recomienda explorar e implementar medidas alternativas menos intrusivas en los sistemas de control de acceso y presencia.

RSM Alert

Diciembre de 2023

CONSIDERACIONES GENERALES

La Agencia Española de Protección de Datos (AEPD), en aplicación de las directrices del Comité Europeo de Protección de Datos emitidas en el mes de abril de 2023, ha realizado una actualización sobre su **Guía sobre Tratamientos de Control de Presencia mediante Sistemas Biométricos**, en la que fija los criterios para el uso de la biometría para el control de acceso, tanto con fines laborales como no laborales, estableciendo las medidas a adoptar para que un tratamiento de datos personales que utilice esta tecnología cumpla con el Reglamento General de Protección de Datos (RGPD).

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

La Guía reconsidera la interpretación que hasta el momento realizaba la AEPD sobre el uso de "Datos Biométricos", concluyendo que en la actual normativa española **no se contiene autorización específica para considerar lícito el tratamiento de datos biométricos con la finalidad de un control de horario de la jornada de trabajo**. De un modo similar, la Guía establece que el consentimiento de los afectados no constituye una condición de licitud para el control de accesos tanto dentro **como fuera del ámbito laboral** (por ej. el control de acceso de clientes a determinados espacios de la empresa). Estos criterios dificultan enormemente la existencia de una base legal que permita levantar la prohibición general del tratamiento de datos biométricos para el control de acceso en la empresa.

En cualquier caso, la Guía precisa que, con carácter previo al inicio del tratamiento, es obligatorio superar favorablemente **una Evaluación de Impacto para la Protección de Datos** en la que se encuentre debidamente justificada la superación del triple análisis de idoneidad, necesidad y proporcionalidad del tratamiento de datos biométricos.

Superados todos los requisitos de cumplimiento del RGPD, en la implementación práctica del tratamiento de control de presencia con medios biométricos, deben implementarse garantías organizativas, técnicas y jurídicas. En particular, al menos han de estar presentes las siguientes medidas por defecto:

- Informar a los trabajadores, o personas si no se está en un entorno laboral, 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.
- Aplicar la minimización de los datos biométricos recogidos, con una evaluación objetiva de que no ha posibilidad de revelar categorías especiales de datos adicionales.
- En el caso de registro de presencia o control de acceso en el ámbito laboral, se deben recoger en los convenios colectivos el conjunto de garantías con relación a estos tratamientos en el sentido dispuesto en el art. 91 de la LOPDGDD.

El efecto de todo lo anterior, es una **clara restricción del uso de medios biométricos**, exigiéndose que para la implementación del tratamiento de control de presencia haya que cumplir con los principios de minimización y de protección de datos, lo que se traduce en la adopción de medidas alternativas equivalentes, menos intrusivas y que traten menos datos adicionales.

Por los motivos anteriores, **resulta imprescindible revisar de forma urgente** los sistemas de control de acceso, presencia y registro de jornada basados en tratamiento de datos biométricos utilizados en la empresa, con el fin de evitar el incumplimiento del RGPD y el riesgo asociado de verse imponer elevadas multas por este motivo.

Acceso al contenido completo de la Guía de control de presencia biométrico en aepd.es

Los criterios recogidos en este documento son comentarios de carácter general y no pueden ser utilizados sin el debido asesoramiento particular. **www.rsm.es** **www.rsm.global** © 2023 RSM International Association. Todos los derechos reservados.

Para más información: ready@rsm.es
www.rsm.es