



La nueva regulación del registro horario en España y sus implicaciones en materia de protección de datos

La nueva regulación del registro horario en España introduce implicaciones importantes en materia de protección de datos, que las empresas deben tener muy en cuenta para evitar sanciones y cumplir con el RGPD y la normativa laboral.

Con la aprobación del nuevo Real Decreto, las empresas deberán revisar sus sistemas actuales de control horario y, en muchos casos, adaptarse o incluso cambiar de proveedor si las soluciones de fichaje que utilizan no están homologadas o no cumplen los estándares técnicos y legales previstos. Los sistemas de registro deberán garantizar no solo la fiabilidad y trazabilidad de los datos laborales, sino también el cumplimiento de todos los principios de protección de datos: licitud, transparencia, minimización, limitación de la finalidad, integridad, seguridad y conservación limitada. De esta forma, el nuevo marco normativo exige una revisión integral de las herramientas tecnológicas empleadas, asegurando que el control horario se gestione de manera proporcional, segura y respetuosa con los derechos de los trabajadores.

En este contexto, resulta imprescindible que las empresas adopten un enfoque estructurado de cumplimiento, revisando tanto sus procedimientos internos como las herramientas tecnológicas empleadas. Para facilitar esta tarea, desde Escura hemos preparado un check-list de cumplimiento que recoge los aspectos esenciales que deben verificarse para asegurar que el registro horario se ajusta a las exigencias del nuevo Real Decreto y al marco del RGPD.

Este listado sirve como guía práctica para revisar la base legal del tratamiento, la minimización de los datos, las medidas de seguridad, los plazos de conservación, la gestión de derechos de los trabajadores y la relación con los proveedores encargados del tratamiento:

1. Base Legal y Finalidad

- Define la base legal para el tratamiento (cumplimiento de obligación legal).
- Limita la finalidad al control horario, sin usos adicionales.

TODAS LAS CIRCULARES DE ESCURA EN NUESTRO BLOG - <https://www.escura.com/es/blog/>



Las circulares de **Escura** tienen carácter meramente informativo, resumen disposiciones que por carácter limitativo propio de todo resumen pueden requerir de una mayor información. La presente circular no constituye asesoramiento legal.

©La presente información es propiedad de **Escura** quedando prohibida su reproducción sin permiso expreso.

2. Principio de Minimización

○ Recoge solo datos imprescindibles: Identificación del trabajador, Hora de entrada y salida, Pausas (si aplica).

3. Seguridad y Confidencialidad

○ Implementa cifrado y control de accesos.
○ Establece roles y permisos claros.
○ Realiza auditorías periódicas.

4. Conservación

○ Mantén los registros 4 años.
○ Garantiza acceso inmediato para: Trabajador, Representantes, Inspección de Trabajo.

5. Sistemas Biométricos

○ Evalúa si son estrictamente necesarios.
○ Realiza Evaluación de Impacto (EIPD) si usas biometría.
○ Considera alternativas menos intrusivas (tarjetas, apps).

6. Derechos del Trabajador

○ Informa sobre el tratamiento a través de un comunicado y establece un protocolo.
○ Permite ejercicio de derechos (acceso, rectificación, etc.).
○ Respeta la desconexión digital.

7. Documentación

○ Actualiza el Registro de Actividades de Tratamiento.
○ Incluye el sistema en el Análisis de Riesgos.

8. Proveedores

○ Firma contratos con encargados del tratamiento.
○ Verifica que cumplen con RGPD.

En Escura recomendamos que estas adaptaciones se aborden cuanto antes y de forma coordinada entre los departamentos laboral y de protección de datos. Las empresas deberán asegurarse de que los nuevos sistemas de registro no solo cumplen las exigencias del Real Decreto, sino también las obligaciones derivadas del RGPD y de la Ley Orgánica de Protección de Datos. De no hacerlo, podrían enfrentarse a sanciones relevantes por parte de la Agencia Española de Protección de Datos (AEPD), especialmente en casos donde se empleen tecnologías invasivas o no se garantice la adecuada protección de la información personal de los empleados.

