30/06/2026

La Agencia Española de Protección de Datos convierte la protección de datos en una pieza clave del ‘compliance’ laboral

La guía de la Agencia exige a las empresas algo más que cumplir la norma: documentar, limitar y justificar cada tratamiento de datos en la relación laboral

La investigación abierta por la Agencia Española de Protección de Datos (AEPD) sobre el uso de la huella digital para el registro horario de los trabajadores de la prisión de Soto del Real demuestra que la protección de datos en el ámbito laboral ha dejado de ser una cuestión formal para convertirse en un verdadero riesgo de compliance. En este contexto, la guía de la Agencia sobre protección de datos en las relaciones laborales, actualizada en diciembre de 2025, ofrece una lectura imprescindible: el control empresarial no puede basarse en la comodidad tecnológica ni en el “por si acaso”, sino en una base jurídica válida, una finalidad concreta, datos mínimos, proporcionalidad y medidas reales de seguridad.

La protección de datos ya no es un asunto accesorio de Recursos Humanos

Durante años, muchas empresas han tratado la protección de datos en el ámbito laboral como un trámite documental: una cláusula en el contrato, una política interna en la intranet y un formulario firmado en el momento de la contratación.

La guía de la AEPD obliga a superar esa visión.

La protección de datos en las relaciones laborales no es una cuestión formal. Afecta al proceso de selección, al contrato, al registro de jornada, a las nóminas, al registro salarial, a los sistemas internos de denuncia, a la videovigilancia, a la geolocalización, al control de ausencias, a la vigilancia de la salud y a la extinción de la relación laboral.

Dicho de forma práctica: allí donde Recursos Humanos toma una decisión, casi siempre hay un tratamiento de datos personales. Y donde hay tratamiento de datos, debe existir una explicación jurídica previa.

“El consentimiento del trabajador rara vez será una base jurídica válida por la posición de desequilibrio existente en la relación laboral”.

El error más habitual: pedir datos “por si acaso”

La AEPD recuerda que el tratamiento de datos personales no puede realizarse por razones de oportunidad, por la facilidad para obtenerlos o porque quizá puedan ser útiles en el futuro. La empresa necesita una base jurídica que legitime el tratamiento.

Este punto tiene una enorme importancia práctica. En compliance laboral, muchas contingencias nacen de formularios demasiado amplios, procesos de selección invasivos, controles empresariales mal diseñados o expedientes internos en los que se acumula información innecesaria.

El problema no es solo tratar datos incorrectos. El problema es no poder explicar por qué se pidieron, para qué se utilizaron, quién accedió a ellos, cuánto tiempo se conservaron y cuándo debieron suprimirse o bloquearse.

Una empresa madura en compliance laboral no pregunta “qué datos puedo conseguir”, sino “qué datos necesito realmente para

esta finalidad concreta".

El consentimiento del trabajador no lo arregla todo

Una de las ideas más relevantes de la guía es que, en el ámbito laboral, el consentimiento del trabajador debe manejarse con extrema cautela. La AEPD recuerda que la base jurídica principal en la relación laboral suele ser la ejecución del contrato de trabajo, no el consentimiento, porque entre empresa y trabajador existe una posición de desequilibrio.

Esta advertencia tiene una consecuencia directa: no todo se soluciona haciendo firmar al trabajador.

En la práctica empresarial todavía se utilizan autorizaciones genéricas para tratar datos, ceder imágenes, usar teléfonos personales, acceder a determinada información o incorporar tratamientos no estrictamente necesarios para la relación laboral.

Ese enfoque es débil. Si el trabajador no puede negarse libremente sin consecuencias adversas, el consentimiento difícilmente será válido. Por eso, el verdadero trabajo jurídico no consiste en acumular firmas, sino en identificar correctamente la base jurídica: contrato, obligación legal, interés legítimo o, solo excepcionalmente, consentimiento.

La minimización es la regla de oro del compliance laboral

La guía insiste en el principio de minimización: los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para la finalidad perseguida.

Para un abogado laboralista, esta regla tiene más importancia práctica de la que parece.

La empresa puede tratar datos necesarios para formalizar y ejecutar el contrato: nombre, apellidos, DNI, número de afiliación a la Seguridad Social, datos bancarios si el salario se abona por transferencia, datos imprescindibles para cotización, fiscalidad o cumplimiento de obligaciones legales. Pero no puede convertir la relación laboral en una autorización general para conocer la vida del trabajador.

La AEPD pone ejemplos muy útiles: no todo dato de contacto personal es exigible; no siempre está justificada la solicitud del correo electrónico o teléfono particular; tampoco puede exigirse información no necesaria para el puesto o para una obligación legal concreta.

La regla práctica es sencilla: cuanto más sensible o periférico sea el dato, mayor debe ser la justificación.

Selección de personal: el primer foco de riesgo

El primer tratamiento de datos suele producirse incluso antes de que exista contrato: en el proceso de selección.

La AEPD recuerda que la empresa solo debe solicitar datos relevantes para el desempeño del puesto y que no cabe una recogida indiscriminada de información. En procesos de selección, las preguntas personales o familiares ajenas al puesto pueden generar riesgos de protección de datos y también de discriminación.

Este punto es especialmente importante para empresas que externalizan selección, revisan redes sociales o utilizan formularios amplios de candidatura.

La guía advierte que las personas candidatas no están obligadas a permitir la indagación empresarial en sus perfiles de redes sociales. Aunque un perfil sea público, la empresa necesita una base jurídica válida para tratar esa información, y la revisión solo se justifica cuando esté vinculada a fines profesionales y resulte necesaria para el puesto.

La enseñanza práctica es clara: un proceso de selección profesional no es el que obtiene más información del candidato, sino el que obtiene solo la información necesaria y puede justificarla.

Registro de jornada y registro salarial: cumplir sin exponer datos innecesarios

La guía también aborda tratamientos especialmente sensibles en la gestión laboral ordinaria, como el registro de jornada y el

registro de salarios.

Estos tratamientos tienen una base vinculada al cumplimiento de obligaciones legales, pero eso no significa que la empresa pueda gestionarlos sin límites. Deben respetarse la finalidad, la proporcionalidad, la confidencialidad y el acceso restringido.

En el registro salarial, la clave práctica es evitar que una obligación de transparencia se convierta en una exposición innecesaria de datos individuales. La empresa debe cumplir sus obligaciones laborales, pero también impedir accesos indebidos, identificaciones innecesarias o difusión interna injustificada.

La transparencia no equivale a circulación libre de datos.

Desde compliance laboral, esto obliga a diseñar procedimientos claros: quién elabora el registro, quién accede, con qué finalidad, cómo se conserva, qué versión se entrega, cómo se protege la información y durante cuánto tiempo permanece disponible.

Control empresarial: la proporcionalidad decide la validez de la medida

El documento dedica especial atención al control de la actividad laboral: acceso a instalaciones, videovigilancia, geolocalización, control de ausencias por enfermedad o accidente y detectives privados.

La AEPD no niega las facultades de control empresarial. Lo que exige es que se ejerzan dentro de los límites de la protección de datos y de los derechos fundamentales.

La empresa debe superar una lógica práctica: la medida debe ser idónea, necesaria y proporcional. No basta con que el control sea útil. Debe ser adecuado para la finalidad, no existir una alternativa menos invasiva y mantener un equilibrio razonable entre el interés empresarial y los derechos del trabajador.

Esta es una de las grandes lecciones para compliance laboral. Antes de instalar cámaras, activar geolocalización, controlar accesos o investigar ausencias, la empresa debe poder contestar preguntas muy concretas: qué finalidad persigue, qué base jurídica invoca, qué datos se recogen, quién accede, cuánto tiempo se conservan, cómo se informa al trabajador y qué medidas menos intrusivas se han valorado.

Si esas respuestas no existen antes de implantar el sistema, la empresa no está haciendo compliance; está creando riesgo.

Sistemas internos de denuncia: confidencialidad no significa improvisación

Los sistemas internos de denuncias, también conocidos como canales de información o whistleblowing, son otro punto crítico.

La guía los incluye dentro del desarrollo de la relación laboral y recuerda que estos mecanismos implican tratamientos de datos especialmente delicados. En ellos pueden aparecer datos de denunciantes, afectados, testigos, directivos, representantes legales o terceros.

Por eso, el canal de denuncias no puede diseñarse como un simple buzón. Debe existir información clara, acceso limitado, trazabilidad, conservación proporcionada, confidencialidad y medidas para evitar represalias o usos desviados. También debe garantizarse que los datos tratados sean adecuados a la finalidad de investigación y que no se acumulen informaciones irrelevantes.

En la práctica, un canal de denuncias mal gestionado puede generar dos problemas simultáneos: un problema laboral por defectos en la investigación y un problema de protección de datos por tratamiento excesivo o inseguro.

Seguridad y confidencialidad: el riesgo también está dentro de la empresa

La AEPD recuerda que responsables, encargados y todas las personas que intervengan en cualquier fase del tratamiento están sujetos al deber de confidencialidad. Además, esa obligación se mantiene incluso después de finalizar la relación con el responsable o encargado del tratamiento.

Este punto suele infravalorarse. La protección de datos no depende solo del departamento jurídico o del delegado de protección de

datos. Depende de todas las personas que acceden a información laboral: nóminas, bajas médicas, expedientes disciplinarios, datos de salud, denuncias internas, evaluaciones de desempeño o documentación sindical.

La AEPD recomienda definir perfiles funcionales, formar al personal y crear una cultura de compromiso con la protección de datos. Esa recomendación es puro compliance laboral.

Una empresa no puede exigir confidencialidad si no ha explicado qué significa, quién puede acceder a qué información y qué consecuencias tiene un uso indebido.

Extinción de la relación laboral: el dato no desaparece con el despido

La finalización de la relación laboral no elimina automáticamente todas las obligaciones de protección de datos.

La guía recuerda la importancia del bloqueo y de la conservación cuando existan obligaciones legales o posibles responsabilidades. La supresión no siempre significa destrucción inmediata. En ocasiones, los datos deben bloquearse para impedir su tratamiento ordinario y conservarse solo a disposición de jueces, tribunales, Ministerio Fiscal, administraciones competentes o autoridades de protección de datos.

La consecuencia práctica es importante: la empresa necesita una política real de conservación y supresión documental. No basta con guardar expedientes indefinidamente “por prudencia”, ni tampoco destruir documentación sin comprobar plazos legales. El compliance laboral exige calendarios de conservación, criterios de bloqueo, responsables internos y procedimientos verificables.

La visión del abogado en ejercicio: la prueba también debe ser lícita

La gran enseñanza de la guía de la AEPD es que el cumplimiento en protección de datos no puede separarse de la defensa laboral.

En un conflicto judicial, la empresa necesitará documentos, registros, comunicaciones, evidencias digitales, informes internos o datos de control. Pero esa prueba solo será útil si se ha obtenido y conservado correctamente.

Por eso, desde la práctica procesal, la protección de datos debe integrarse en cada decisión laboral relevante: contratación, promoción, sanción, despido, investigación interna, control horario, teletrabajo, uso de dispositivos, videovigilancia, salud laboral y denuncias internas.

El abogado laboralista moderno no puede limitarse a preguntar si la empresa tiene razón. Debe preguntar también cómo ha obtenido los datos con los que pretende demostrarla.

Conclusión: el compliance laboral se demuestra en el tratamiento diario de datos

La guía de la AEPD confirma que la protección de datos en la empresa no es una materia aislada ni meramente tecnológica. Es una parte esencial del compliance laboral.

Su mensaje práctico puede resumirse así: la empresa debe tratar datos personales de trabajadores solo cuando tenga una base jurídica válida, una finalidad concreta, datos necesarios, información clara, acceso limitado, seguridad suficiente y plazos definidos de conservación.

El incumplimiento no suele nacer de grandes decisiones estratégicas, sino de prácticas cotidianas: pedir más datos de los necesarios, revisar redes sociales sin base jurídica, usar teléfonos personales sin justificación, conservar expedientes sin criterio, permitir accesos amplios a nóminas o implantar controles laborales sin proporcionalidad.

Ahí es donde se gana o se pierde el verdadero compliance laboral.

La empresa que quiera reducir riesgos no debe limitarse a tener documentos. Debe poder demostrar que sus procedimientos funcionan.

Llamada a la acción

Las empresas deben revisar sus procesos de Recursos Humanos desde la óptica de la AEPD: selección, contratación, control horario, registro salarial, canales de denuncia, videovigilancia, geolocalización, conservación documental y extinción contractual. El compliance laboral efectivo no consiste en tratar más datos, sino en tratar los datos correctos, con base jurídica, finalidad clara, proporcionalidad y medidas de seguridad suficientes.

Además, la gestión ilícita de datos personales no solo puede generar sanciones administrativas o riesgos reputacionales. También puede tener una consecuencia procesal decisiva: que los datos obtenidos o tratados de forma ilegítima sean declarados nulos como prueba en un procedimiento judicial si vulneran un derecho fundamental del trabajador. Por eso, antes de utilizar cualquier evidencia laboral, la empresa debe preguntarse no solo si esa prueba le resulta útil, sino si ha sido obtenida de forma lícita, proporcionada y defendible ante un juez.

Fuente: La Agencia Española de Protección de Datos convierte la protección de datos en una pieza clave del 'compliance' laboral | E&J