



La AEPD publica una guía sobre protección de datos y relaciones laborales

La guía ha sido elaborada por la Agencia con la participación tanto del Ministerio del Trabajo como de la patronal y organizaciones sindicales

La Agencia Española de Protección de Datos (AEPD) ha publicado la guía '[Protección de datos y relaciones laborales](#)' con el objetivo de ofrecer una **herramienta práctica** de ayuda a las organizaciones públicas y privadas para un adecuado cumplimiento de la legislación. Esta guía ha sido elaborada por la Agencia con la participación tanto del Ministerio del Trabajo y Economía Social como de la patronal y organizaciones sindicales.

La aplicación del Reglamento General de Protección y la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDGDD) ha supuesto una serie de cambios tanto en lo relativo a los derechos de las personas trabajadoras como en la recogida y el uso de sus datos por parte de los empresarios. Asimismo, la guía también aborda temas que se plantean cada vez con mayor frecuencia, como la consulta por parte del empleador de las redes sociales de la persona trabajadora, los sistemas internos de denuncias (whistleblowing), el registro de la jornada laboral, la protección de los datos de las víctimas de acoso en el trabajo o de las mujeres supervivientes a la violencia de género o el uso de la tecnología wearable como elemento de control.

El documento comienza recogiendo las **bases que legitiman el tratamiento** de datos personales, la información que es necesario facilitar y los derechos de protección de datos aplicados al entorno laboral. Aborda también el **principio de minimización**, ya que la ejecución del contrato de trabajo no implica que el empleador pueda conocer cualquier tipo de dato personal de las personas trabajadoras. Además de los **deberes de secreto y seguridad** (que los datos personales sólo sean conocidos por el afectado y por aquellos usuarios de la organización con competencias para usar, consultar o modificar esos datos), el documento también recoge los límites al tratamiento de datos en los procesos de selección y contratación de personal.

En el apartado de **selección de personal y redes sociales**, la Agencia detalla que las personas no están obligadas a permitir que el empleador indague en sus perfiles de redes sociales, ni durante el proceso de selección ni durante la ejecución del contrato. Aunque el perfil en las redes sociales de una persona candidata a un empleo sea de acceso público, el empleador no puede efectuar un tratamiento de los datos obtenidos por esa vía si no cuenta para ello con una base jurídica válida y para ello será necesario informar de ello a la persona trabajadora y demostrar que dicho tratamiento es necesario y pertinente para desempeñar el trabajo. Por otro lado, la Agencia aclara que la empresa no está legitimada para solicitar 'amistad' a las personas candidatas para que éstas proporcionen acceso a los contenidos de sus perfiles.

En cuanto a los **sistemas internos de denuncias o whistleblowing**, la Agencia considera que la información tanto a los denunciantes como a los potenciales denunciados reviste un carácter primordial. La LOPDGDD admite sistemas de denuncias anónimas y, en caso de que la denuncia no sea anónima, la confidencialidad de la información del denunciante debe quedar a salvo y no debe facilitarse su identificación al denunciado. Además, el personal con funciones de gestión y control de recursos humanos sólo podrá acceder a dichos datos en caso de procedimientos disciplinarios, sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo.

En lo referente al **registro de jornada obligatorio**, la Agencia recomienda que se adopte el sistema menos invasivo posible y este no puede ser de acceso público ni estar situado en un lugar visible. Asimismo, los datos de ese registro no pueden utilizarse para finalidades distintas al control de la jornada de trabajo, como comprobar la ubicación. Es el ejemplo de una persona trabajadora itinerante cuyo registro de jornada se realiza por geolocalización. La finalidad ese registro es comprobar cuándo comienza y finaliza su tiempo de trabajo pero no verificar dónde se encuentra en cada momento, ya que el tratamiento de datos de geolocalización requiere de una base jurídica específica.

La guía también incorpora una novedad relevante sobre el derecho del comité de empresa a ser informado por la empresa de los **parámetros en los que se basan los algoritmos o sistemas de inteligencia artificial**, incluida la elaboración de perfiles, que pueden incidir en las condiciones, el acceso y mantenimiento del empleo. Esta novedad, aprobada en el reciente RD-ley 9/2021, que modifica el Estatuto de los Trabajadores, constituye un precedente de transparencia adicional a las garantías de la normativa de protección de datos.

Otro de los aspectos que aborda el documento es la difusión de las **ayudas concedidas por acción social**, especificando que las empresas no pueden publicar el listado de ayudas adjudicadas y denegadas en una página web de libre acceso, o en un tablón de anuncios situado en una zona abierta al público. En el caso de que las ayudas se vinculen con categorías especiales de datos (por ejemplo, ayudas por hijos con discapacidad) la publicidad de la concesión de la ayuda no ha de permitir la identificación del afectado.

La guía 'Protección de datos y relaciones laborales' también aborda la **protección de la privacidad de las víctimas de acoso en el trabajo y de las mujeres supervivientes a la violencia de género** y determina que sus datos personales y en particular su identidad, tienen, con carácter general, la consideración de categorías especiales de datos personales y, en todo caso, son datos sensibles que exigen una protección reforzada. Así, recoge que deberá asignarse un código identificativo tanto a la persona supuestamente acosada como a la acosadora, con objeto de preservar la identidad de estas. Además, el empleador podrá conocer y tratar los datos de una trabajadora vinculados a la condición de mujer superviviente a la violencia de género cuando resulte necesario para el cumplimiento de las obligaciones legales pero, en todo caso, la documentación de la empresa debe incluir un código que no permita que terceros puedan asociar esa información con la trabajadora.

La Agencia también aborda en la guía la **tecnología wearable**. La AEPD indica que monitorización de datos de salud a través de dispositivos inteligentes, como pulseras o relojes, está, por lo general, prohibida, a menos que esté establecida por ley o reglamentariamente, dado que no se enmarca en la vigilancia de la salud propia de la prevención de riesgos laborales, supone el tratamiento de una categoría especial de datos (salud) sin una base jurídica, no cuenta con una finalidad legítima y vulnera el principio de proporcionalidad, dado que conlleva una monitorización permanente y permitiría al empleador acceder a datos de salud específicos, y no exclusivamente a la valoración sobre la aptitud para desempeñar el trabajo.